International Journal of Engineering & Technology, 7 (4) (2018) 3521-3529

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.17790
Research paper

Secured reversible color image data hiding technique using image classifiers and Lempel-Ziv-welch image compression technique

Anitha Devi M.D [1] *, K.B. Shiva Kumar [2]

[1] Electronics and Communication Engineering , SSAHE, Tumakuru, India
[2] Telecommunication Engineering , SSAHE, Tumakuru, India
**Corresponding author E-mail: anumdssit@gmail.com*

Abstract

Recent advancement in data transfer and networking techniques has put forward a considerable threat for secure data transfer. It is the sensitive information that flows via network fuels the engine of global economy. One of the main concerns in data communication is the ability to exchange information in a secured fashion and embed the information of interest in any multimedia carrier like audio, video and an image. The proposed work is an ideal modernistic novel approach for secured sensitive information communication over an encrypted color host image carrying exceptionally confidential data. Distortion less retrieval of both payload and host signal information from marked image is an appealing feature in scenarios like medical, Military and satellite applications. Reversibility not only assures zero error retrieval of sensitive information hidden and also perfect reconstruction of host medium information contents while safeguarding the confidentiality of secret information. Most popular and widely in use Advanced Encryption Standard(AES) stream cipher in Counter mode is used for encrypting the cover image content, by performing XOR operation over cover image information bits with key dependent pseudorandom bits. Signal Processing over the encrypted domain is one of the most demanding features for most of the privacy preserving applications like cloud computing and remote sensing. High Embedding capability is achieved through Lempel-Ziv-Welch (LZW) compression technique. High performance reversible data hiding technique is assured via public key modulation scheme. Two of the most powerful image classifiers Support Vector Machine (SVM) and K- Nearest neighbor (KNN) algorithms are used at the decoder end to distinguish between encrypted and non encrypted image blocks. Performance evaluation of image classifiers is done, considering their ability to accurately categorize image patches as encrypted and unencrypted using feature vectors. Features used for categorizing encrypted and unencrypted image blocks are variation of pixel intensity in all four directions, entropy, standard deviation and histogram plot of segmented image blocks. Proposed algorithm comes with a unique feature of simultaneous retrieval of both host image and payload information in an error free fashion with zero distortion. Proposed algorithm is proven more secured considering several security attacks as evaluation parameters. Few of Cryptanalysis and Steganalysis techniques considered to verify the security feature of proposed algorithm are Sample pair analysis (SPA), Number of changing pixel rate (NPCR), Unified averaged changed intensity (UACI) and Chi-square attack.

***Keywords**: AES Stream Cipher; Chi-Square Attack; Correlation; Entropy; Histogram; KNN Classifier; LZW Compression; NPCR (Number of Changing Pixel Rate); Public Key Encryption; Reversible Data Hiding; SVM Classifier; SPA (Sample Pair Analysis); UACI (Unified Averaged Changed Intensity).*

1. Introduction

1.1. Motivation

Recent advancement in the field of information transfer and networking has put forward a considerable threat to secure data transmission. Hence there is a lot of scope for the researchers in the field of covert communication during recent years. Reversible covert communication algorithms are special type of data hiding techniques, which results in perfect reconstruction of host medium information after extracting the secret information hidden within. This is one of the most demanding features in applications such as law forensic, satellite communication, medical and military applications. Most of the existing reversible covert communication techniques do not assure perfect reconstruction of carrier image information. I.e. host medium information loss cannot be avoided, as the host image pixel contents are replaced with sensitive secret information bits. During recent years covert communication over an encrypted domain is the most demanding feature for privacy preserving applications like cloud computing and secure remote sensing. Since the third party who processes the sensitive image data are usually not trusted. To ensure the security of host image contents, it will be encrypted before being transmitted via communication channel to data center for additional processing. Data centre is not aware of undisclosed key agreed upon prior to transfer of information between two communicating parties. This results in reliable key administration. In this proposed technique, host medium is encrypted by using advanced encryption standard cryptographic algorithm in counter mode.

1.2. Methodology

- Studying the existing models of data hiding techniques like steganography, Cryptography and Watermarking.
- Testing the existing methods for their results and analysis.

- Developing and/ or improving the existing models for better results and better performance.
- Developing new methods of data hiding, simulating and testing for better performance using available simulation tools and software packages.

Encryption of Host signal: To protect confidentiality of host signal, it is encrypted using AES (Advanced Encryption standard) stream cipher in CTR mode [1]. AES Stream cipher in CTR mode is an attractive encryption algorithm, which uses Advanced Encryption Standard cipher to generate encrypted data. Information is Encoded and decoded by simple reversible XOR operation with a bit stream of key produced by AES cryptographic technique in counter mode, encrypting sequential counter block values. AES-CTR also supports pre computation of key stream.

LZW Compression technique: Lempel-Ziv-Welch (LZW) data compression algorithm is worldwide accepted data compression algorithm. To ensure greater data hiding capability, payload information is initially compressed using LZW compression algorithm. LZW compression is the compression of a file into smaller file using table based lookup algorithm. LZW data reduction algorithm reduces the number of information bits by generating an entry in lookup table called as dictionary for a particular bit pattern, consisting of the pattern itself and a code which is shorter in length. As and when input sequence is read, any pattern that has been read earlier will result in substitution of shorter codes, thereby reducing the amount of data for representing the actual information. The decoder which de compresses the file will build the table by itself by using the algorithm, when it processes the encoded compressed data input.

Public Key Encryption table for data hiding [16]:

Public key cryptography is a form of data encryption where in the key used to encode information is different from the key used to decode it. Public key cryptography uses two keys i.e. public key and private key. The private key is kept secret, while the public key is widely distributed. In the Proposed algorithm, Number of public keys depends upon number of bits to be hidden in every sub block of encoded host image. Table 1.1shows the public key encryption table for n=3 , If n is the number of bits to be hidden in each divided block of size 8X8, then the number of public keys is equal to 2^n and the key size is 64.

Table1.1: Public Key Encryption Table for N=3

	1	2	3	…	…	63	64
E1	9	88	59	…	…	129	251
E2	25	19	26	…	…	11	33
E3	69	92	89	…	…	96	184
E4	25	47	55	…	…	88	150
E5	129	147	169	…	…	198	156
E6	66	97	126	…	…	110	165
E7	255	39	42	…	…	57	95
E8	05	63	13	…	…	252	55

For example: If n=5, then number of public keys=2^5=32 keys

Table1.2: Public Key Encryption Table for N=5

	1	2	3	…	…	63	64
E1	155	10	55	…	…	123	251
E2	25	19	23	…	…	10	33
E3	66	69	94	…	…	99	111
E4	21	48	53	…	…	89	119
E5	127	149	190	…	…	180	194
…	7	11	92	…	…	00	60
E31	85	77	44	…	…	59	69
E32	99	67	77	…	…	200	85

Ref [4] As shown in Table1.2 ,If n=5, then number of public keys=2^5=32 keys and If the size of fragmented block is 7X7, then the key length is 49 bytes , Rules to be followed while generating the public key encryption table are

i) No elements in each row should be repeated.
ii) No row of matrix should be repeated
iii) The values of encryption matrix are the values representing different grey levels from zero to two fifty five.

Image Classifiers:

In supervised image classification, the analyst will supervise the pixel characteristics. Analyst specifies the various pixel values associated with each class. This is done by selecting appropriate training sets. Then the classification algorithm uses special signatures from these trained features to classify the image blocks into different classes.

The following steps are followed in a supervised image classification technique

i) Analyst collects training data.
ii) Analyst specifies the features to be used for classification.
iii) Algorithm assigns pixels to closest class based on trained features.
iv) Classification is made based on evaluation of result.
v) Support Vector machine (SVM) [1]:

SVM is one of the most popular supervised machine learning algorithms used for categorizing. Support vector machine uses the idea of finding a appropriate hyper plane that categorizes the information in a best way into different classes. Figure 1.1 shows graphical plot of SVM classifier. Support vectors are the critical elements of a dataset; they are the feature elements nearest to the hyper plane. If these points are varied, it would alter the position of dividing hyper plane. The distance between the hyper plane and the nearest trained feature value is known as safe margin. The main aim is to choose a hyper plane with the greatest possible margin between the training feature set and the hyper plane, so that there is a greater chance of data being classified accurately.

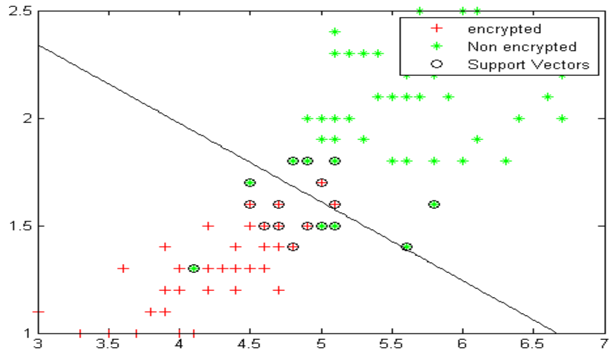


Fig 1.1: Output of Two Class Linear Image Classifiers.

K-Nearest neighbor (KNN):

KNN algorithm widely used in pattern recognition is used for categorizing image blocks. Here information consists of K closet examples used for training in the feature space. The output in KNN classification is a class membership. If an element is classified by a majority of votes from its nearest neighbors, for example if k is assigned with a value 1, then the element is simply assigned that class of single nearest neighbor. In KNN algorithm weights associated with each object is reciprocal of distance d to the neighbor, so that adjacent elements donate largely to the average than the farer ones. The adjacent elements are those whose class or the object property value is known. These set of values are used for training and no explicit training for classifier is required. The best way to choose K depends on nature of the data, but larger values of K make barriers between the classes less specific.

Security attacks [17]:

AES Stream cipher is proven more secured against differential cryptographic attack. Differential cryptanalysis is usually a chosen plain text attack. It means that the hacker will try to generate cipher texts for some set of plaintext. The basic method is choosing a pair of plaintext, which is related by a constant difference in values. Usually exclusive OR operation is chosen as the difference. The hacker finds differences of corresponding cipher texts, planning to identify the statistical approach in distribution. The resultant pair of differences is known as differential. The AES non linear function has highest differential probability.

Security Evaluation Parameters:

i) NPCR (Number of changing pixel rate) and UACI (unified averaged changed intensity): The two of the most widely used parameters to evaluate the effectiveness of the algorithm in terms of its security are NPCR and UACI. These two security attacks are mainly designed to test the number of changing pixels and the average intensity change between original image and cipher image. If C1 represents cipher text image before one pixel change and C2 represents cipher text image after one pixel change, then the pixel values of corresponding images at (p, q) is C1(p, q) andC2(p , q) as represented in equation 1.6.1

$E (p, q) = 0$, if $C_1 (p, q) = C_2 (p, q)$

$E (p, q) = 1$, if $C_1 (p, q) \neq C_2 (p, q)$ (1.6.1) ref [17]

Let S denote total number of pixels in the encoded text and let P denote the largest pixel value compatible with the encoded text image. Then equations to find NPCR and UACI are as shown in equations 1.6.2 1nd 1.6.3.

$NPCR = \Sigma_{p,q} E(p , q)/S*100\%$ (1.6.2) ref [17]

$UACI= \Sigma_{p,q}| C_1(p ,q) - C_2(p ,q)| / (P*S)$ (1.6.3) ref [17]

A greater value of number of changing pixel rate is analyzed as greater opponent to differential attacks and UACI measure helps to identify the average intensity of difference in pixels between the two images. The range of UACI is between 0 to 1. NPCR and UACI are random variables dependent on parameters such as image size and format of image.

Chi-Square attack [4]:

It is one more widely used security evaluation parameter to evaluate effectiveness of any steganographic algorithm. It is based on frequency with which pixel value appear. Chi square goodness of fit test is a non parametric testing technique used to find out how far the observed value of a given set of data is significantly different from the expected value. The probability of data hiding is near to ONE, if the image is likely to have hidden information and is near to ZERO, if it is unlikely to have hidden information.

Sample pair analysis (SPA):

This analysis indicates the uniqueness of data values. High uniqueness indicates that in each column there is high percentage of totally cardinal values. Low uniqueness indicates that each column has lot of repeats in its data range. The method is based on finite state machine. States of FSM are simple pairs having multiple sets.

1.7: Feature Selection for discriminating encrypted and non encrypted image blocks

To differentiate encrypted and original unencrypted image blocks, we here design a feature vector

F = (E, H, σ, v1, v2, v3, v4), integrating the characteristics from multiple perspectives. Here, H is the histogram of an image block, E is a tailored entropy indicator, σ is the standard deviation of the block, and v1, v2, v3, v4 represents the directional local complexities in all four directions. The formation of the above feature elements will be detailed as follows.

ii) Entropy (E) [5]: The entropy is a parameter which is used to measure the randomness of the fragmented block. It is a scalar value. It gives the information regarding texture of an image. For encrypted blocks, the randomness between the pixels will be more, thus the entropy value should be high and for non-encrypted blocks, the randomness between the pixels will be less, and thus the entropy value should be less. The entropy indicator E based on quantized samples is then given by the equation 1.7.1

$$E= -\Sigma (P_i \log P_i) \qquad (1.7.1)$$

Where P_i is the empirical probability of i in the quantized block.

iii) Standard Deviation (σ)[8]: This parameter represents how far the individual pixel values differ from mean value of pixels. The neighboring pixel value remains almost same for the plain image or non-encrypted image, thus by calculating the mean and variance, the variance value should be less. Since the pixels values are not same in the encrypted image, the variance value should be high.

Standard deviation of an image block can be calculated using equation 1.7.2.

$\sigma = \sqrt{}\ (1/m*n)\ \Sigma(p(i)-\mu)^2$ 1.7.2 ref [1]

Where p(i) is the i^{th} pixel in the block and

$\mu= (1/m*n)\Sigma_i\, p(i)$ is the sample mean over all the samples in the block. By including this feature element, we can improve the classification performance, as the data depressiveness and denseness can be better reflected.

iv) Histogram (h) [12]: A histogram is an accurate graphical representation of the distribution of numerical data. For encrypted blocks, the probability of occurrence at each pixel will be uniform and thus histogram graph should be flat and for non-encrypted blocks, the probability of occurrence at each pixel will be non-uniform, thus histogram graph should be non-uniform.

v) Directional Features (V) [1]: In addition to the above feature components, a directional complexity indicator is included that encode the local geometric information. This parameter represents pixel variation in all four directions. To this end, we define a four-element vector, V = (v1, v2, v3, v4), as defined in equation 1.7.3.

Where $v1= \Sigma_i|p(i)-p(i)_{ne}|$, $v2= \Sigma_i|p(i)-p(i)_e|$,

$v3= \Sigma_i|p(i)-p(i)_s|$, $v4= \Sigma_i|p(i)-p(i)_{se}|$ ……1.7.3 ref [1]

Where p (i) is the pixel value.

The organization of this paper is as follows.

In section 2, we discuss previous existing works based on Reversible data hiding approaches over encrypted domain. Proposed algorithm is discussed in section 3. Results and discussion along with plots of various experimented results and comparing the proposed algorithm with existing implemented techniques in section 4, Conclusion and future scope in section 5.

2. Related work

In Literature, researchers have put forward several good Reversible covert communication algorithms taking into consideration several parameters of information safety and distortion less recovery of host medium contents. Looking into the need for Reversible lossless covert communication techniques for critical applications with sensitive information, Researchers have proposed several secret communication algorithms considering distortion less recovery of carrier and secret medium information.

Jiantao Zho et.al [1] has proposed a reversible secret data communication technique over an encoded host medium. A two class Support Vector Machine classifier is used to classify input image patches as encrypted and unencrypted picture segments. The efficiency of this proposed technique is verified considering various evaluation parameters with grey scale image being the host image. But the proposed work is implemented for gray scale image and the amount of information embedded is less since no compression algorithm is applied to payload information prior to embedding.

X.Zhang et.al [2] has proposed a RDH scheme for an encrypted image with least computational complexity. At the decoder side, using correlation in the spatial domain in natural image, the embedded information can be recovered and host image could be retrieved without any loss in information. But in the proposed technique error free recovery of both cover and payload is not achieved. PSNR value is less when compared to our proposed technique.

Wein Hong et.al [3] has proposed a RDH scheme which is an improved version of [2]. This technique uses an improved data hiding technique to measure the smoothness of fragmented image block. It adopts side match technique to decrease the error rate of extracted information. Main drawback of proposed technique is mean square error is not zero unlike our proposed technique

Soria-Lorente et.al [4] proposes a data hiding technique using JPEG compression standard and an entropy threshold technique. Embedding is done at the first seven coefficients in the transformed domain using DCT. The proposed algorithm is proven resistant to chi square attack. In this proposed algorithm the amount of compression achieved is less in comparison with our proposed LZW compression technique.

L. Velasco-Bautista et.al [5] proposes a steganographic technique of covert communication based on discrete cosine transform and entropy threshold technique. In this proposed algorithm, a random function is used to select block of image, where in the bits of secret information is inserted. Insertion is done in low frequency AC coefficients of the block. Proposed algorithm is proven secured considering relative entropy as the parameter. In this proposed algorithm security is evaluated considering only entropy as the evaluation parameter. In our proposed algorithm both cryptographic as well as steganographic attacks are considered as evaluation parameters to evaluate secured feature of covert communication technique.

Mehmet et .al [6] has put forward a distortion less LSB information embedding algorithm which results in perfect rebuilding of the host image contents after retrieving the secret information but results in some error between the host and payload image. For few images, this technique results with sufficient embedding capability, which is the desired feature in several applications. For example, in implementations where in there is a need for very high data embedding capability, this algorithm can be altered to adjust the data hiding parameters to satisfy the greater embedding need, and hence compromising with in-between loss of data with higher embedding capability. The algorithm proposed is proven to exceed bit-plane data reduction and RS information embedding techniques, usually for average to high erroneous patches. But hundred percent PSNR is not achievable with LSB embedding technique.

Mehmet et.al [7] has put forward a covert communication technique for distortion less genuine data hiding algorithm, which ends with perfect retrieval of the un-encoded segments of image. The proposed method lets evaluation of the marked picture information before retrieval of host picture information, but in existing techniques, there was a need for extraction of the host image before it could evaluate the marked image. This would end with reduction of complication in computation, where in either the validation stage is unsuccessful or the perfect retrieval is not required. For evaluated image patches, the retrieved picture information is promised with distinct rebuilding technique. This method proves a particular application technique using hierarchy based image validation and error free data embedding technique. Amount of information embedded is less and security feature is not evaluated considering various attacks.

Puech et.al [8] has developed a reversible covert communication technique over encoded images where they are capable of hiding the secret information in encoded image patches and then decoding of the image is carried out; at the decoder end, the host image is retrieved back by extracting back the secret information. This algorithm uses standard deviation of the marked encrypted image patches to remove the hidden information at the decoder. Thus it is made secured with encoding or information embedding techniques. The information need to be compressed to decrease the transmission time. In proposed technique encoded data compression, and information embedding is done in only one step. Embedding capacity is less in comparison with our proposed technique.

Yongjian Hu et.al [9] have developed a reversible data embedding technique based on Difference Expansion with improved overflow location map. The embedded sequence of information mainly has two components: the first part is the secret information while the rest of the portion is the auxiliary message bits for blind detecting technique. To enhance the information embedding capacity, the suggested method concentrates on improvement of the overflow location map which is mainly dependent on the payload data. It works efficiently for different image types, acquiring better data hiding capacity and better quality of image restored with less distortion. Error free retrieval of Host image is not achieved with proposed technique.

Xinpeng Zhang et .al [10] has developed a reversible information embedding technique with best value transmission by identifying the best equivalent value transmission matrix by enlarging a required function of payload data with an iterative technique and recommends a lossless data hiding method. The difference in between the original pixel value and the picture element information predicted from the adjacent pixels are made use of to embed the secret data. The host picture information is categorized into several sub picture elements and the auxiliary data of subset is embedded into the estimated differences in the upcoming sub picture elements. At the receiver end, we can extract the secret information and retrieve the host medium contents in the sub blocks in reverse fashion. The best transmission method provides a novel method of picture element value manipulation and could be used on various cover image contents. If an improved approximation technique is used to predict differences nearer to null, an improved performing can be achieved. But the limitation is larger complexity in computation.

Xinpeng et.al [11] has developed a reversible data hiding method in ciphered host medium. The host image elements are initially encoded by a stream of cipher bits. With marked medium, the receiver will first decode it using the appropriate key, and the decoded information is very similar to the host image with very minimal error. Zero mean square error is not achieved with this proposed technique

Xiaolong et.al [12] has developed an error free information embedding algorithm considering histogram manipulation using mapping of difference pair. In this proposed technique, taking into consideration pair of pixel values and its data, a sequence having a pair of difference value is identified. As a next step, difference in the histogram of a two dimensional matrix is developed by finding the number of occurrence of the difference pairs obtained. At the end, reversible information embedding is developed in accordance with difference pair mapping method. Here, the deformable parts model is a relative mapping defined on pairs of difference. A picture element pair of values choosing technique is utilized to embed data. Rate of embedding capacity is less in comparison with our suggested technique

Ma et.al [13] has developed a reversible information embedding technique over an ciphered picture by using a method known as “Reserving the room before encryption”. During recent days Reversible Information embedding schemes over ciphered images is in high demand, since it comes with unique feature that the host medium information can be extracted with less error after payload information is recovered while safe guarding the host medium information content's confidentiality. The suggested technique is proven efficient for the information embedded to reversibly hide the data in the ciphered host medium. Host medium is a grey scale image and our suggested technique is implemented for color host images.

Qian et.al [14] has developed a reversible information hiding algorithm over a ciphered host medium of Joint Photographic Expert Group format. The suggested technique focuses on encryption of a JPEG sequence bits into a well arranged several structure images and embedding payload data into the ciphered JPEG host medium by altering the JPEG bit sequence. The sensitive data bits are ciphered with error correction codes, which results in a distortion less information recovery and host medium recovery. If receiver has all the keys, the secret sensitive data contents could be recovered by observing the articrafts of the blocks of the neighboring image patches, and the original Joint Photographic Expert Group host sequence of bits is retrieved with minimal error. In case the receiver has only one key i.e. the key with which the data is encrypted, it will still retrieve the sequence of information bits to recover the host medium with least error without the need for extraction of payload data. The effectiveness of the proposed algorithm is not evaluated considering various security attacks.

Anitha Devi M.D et .al [15] has developed a histogram shifting based information embedding algorithm which is reversible with quad tree decomposition technique used to identify the redundancy within color cover medium. Algorithm efficiency is evaluated considering PSNR and embedding capacity as the evaluation parameters. The amount of data embedded is less in the above suggested algorithm.

Anitha Devi M.D et.al [16] has suggested a information embedding algorithm which is reversible over color carrier encrypted domain using SVM classifier. Reversible communication is achieved through embedding secret information within host media using public key modulation. In the proposed algorithm both text and image is considered as payload information. Classifier accuracy is compared with existing techniques. KNN classifier is proven more error free in comparison with SVM classifier with our proposed technique. The algorithm is not evaluated in terms of its security considering various attacks.

Yue Wu et.al [17] has proposed several security evaluation parameters to verify the efficiency of data hiding algorithm in terms of security. NPCR and UACI are the evaluation parameters discussed in detail to verify the effectiveness of any data hiding algorithm. Cryptographic attacks are not considered for evaluation of security in this proposed algorithm

Sorina Dumitrescu et .al [18] has proposed detection of LSB Steganography via Sample Pair Analysis , which is one of the evaluation parameter to evaluate the effectiveness of data hiding algorithm in terms of security. Major drawback of this proposed algorithm is error free recovery of both host and secret information media is not achieved.

John Babu et.al [19] proposes a survey of various steganalysis techniques available in literature. A detailed survey of existing hacking techniques is done considering different filtering based preprocessing methods, feature extraction methods and machine learning based classifying techniques for the correct identification of hidden information embedded within host image.

Brinda Murugan et.al [20] proposes image encryption scheme based on chaos using Lorenz equation with different levels of diffusion and Henon mapping. The Henon method is used for creating confusion in the host image and Lorenz equation for diffusion of secret information. The proposed technique is proven secured considering NPCR and UACI as steganalysis evaluation parameters. Cryptographic attacks are not considered for evaluation.

X. Li et.al [21] proposes prediction error expansion based reversible watermarking, which provides high embedding capacity by incorporating prediction error expansion strategies, i.e. adaptively hiding one or two bits into pixels expandable based on local complexity. The effectiveness of the algorithm is evaluated experimentally considering PSNR and capacity as the evaluation parameters. Security attacks are not considered for evaluation of proposed algorithm.

T. Bianchi [22] proposes signal processing technique over encrypted domain. Signal processing using discrete Fourier transform is carried out over the encrypted domain using homomorphism properties of the underlying cryptosystems. Several of the issues are considered for DFT using direct method, Radix-2 and Radix-4 FFT algorithm including the error analysis. The evaluated results prove that Radix-4 FFT algorithm is best suitable for signal processing over encrypted domain in the proposed algorithm.

Z. Erkin [23] proposes a mechanism to protect highly sensitive private information against the service provider, while retaining the actual functioning. Randomness is created by initially encrypting the sensitive information and processing them under encryption. A highly effective technique that does not need participation of the user in an active manner is developed by introducing semi trusted third party and using data packing. Evaluated results prove that proposed algorithm lets a way to produce private recommendations in a privacy preserving way. But amount of data hidden within host medium is less.

B. Yang [24] recommends information embedding technique which is reversible over a ciphered domain. The payload information is initially modulated using different encryption keys. At the decoder side, different decoded information are verified considering typical distribution of randomness in time and frequency domain and the goodness of fit degrees are compared to extract one hidden bit. Proposed algorithm yields better results for natural and textual images, both in grey level and binary bits. Only gray scale images are considered as host medium.

F. Cayre [25] proposes a theory of security to watermarked media based on cryptanalysis. The security provided to data hiding algorithm, is defined in terms of number of observations the hacker needs to make to successfully estimate the secret key. This theory in the proposed algorithm is applied to two of the most popular watermarking techniques like substitutive and spread spectrum based techniques. Their security levels are calculated considering different attacks. Even though algorithm is proven secured, it does not result with hundred percent PSNR being achievable.

M. Barni [26] proposes an algorithm focusing on developing an automatic privacy preserving application, where in remotely placed server classifies a biomedical signal provided by the server without getting any information about the biomedical signal and the final result of classification. The proposed technique deals with all the requirements related to working with biomedical information like Electrocardiogram (ECG). The proposed algorithm verifies that doing complex operations like Electrocardiogram categorization in the encoded domain effectively is only possible in the semi honest built model, which provides the way for some very interesting further enhancements. In this proposed algorithm, ECG signal is considered for classification unlike our proposed technique where in we use colour images as the medium.

3. Proposed method

Step1: Feature extraction of cover images for classification: Support Vector Machine and K-Nearest Neighbor technique are two of the very popular image classification techniques used. Categorization into two different classes is defined in the following steps

1) Identifying the different classes for classifying: In our proposed algorithm, two classes are defined. They are encrypted and unencrypted image patches.
2) Identifying the features for selection: Seven features of the trained cover images are used for classifying. They are

i) Picture element differences in all four direction being labeled as (v1, v2, v3, v4).
ii) Entropy, which indicates quantitatively randomness defined statistically, which is equivalent to input image texture, it is labeled as “E”.
iii) Standard deviation, projects how nearer or far the individual picture element responses deviate from the mean. It is labeled as “σ”.
iv) Histogram representations, which is a graphical way of denoting the tonal variation of a picture. It is labeled as “H”. So totally, the vector used for representing the feature elements for categorization is F = [E, H, σ, v1, v2, v3, v4].

Step2: Carrier image Encoding: Steps for encoding carrier image:

i) Choose any carrier image of size 512x512.
ii) Generate any random encryption key agreed upon between two communicating Parties.
iii) Read the input carrier image pixel values.
iv) If the carrier image is color image, then split the image into three different planes. R, G, B. Individual planes are encrypted separately.
v) To encrypt the carrier image, image pixel values are XOR ed with encryption key.
vi) Resultant image is encrypted carrier image.

Step 3: Lossless compression of secret information bits

Payload information bits are compressed in a error free manner using LZW (Lempel–Ziv-welch). This would result with added greater hiding capability in comparison with already existing algorithms. Resultant payload image is compressed sensitive data bits in an error free manner.

Step 4: Embedding Payload information bits within carrier medium

i) Encrypted carrier image is divided into series of non overlapping blocks of any random size 8x8, 4x4, 5x7 etc. Number of pixels in each divided blocks is equal to number of columns in public key encryption table.

ii) In each of the divided blocks , if n bits of payload information need to be hidden then number of rows of public key encryption table is equal to 2n and number of pixels in each divided block is equal to number of columns of public key encryption table. If n=4, then the lookup table is having totally 16 keys. If the block size is 64, i.e. 8x8 block size, then the key size of each is 64 bytes. All the public keys are predefined in data embedding algorithm.

iii) Reduced secret information is modified into sequence of information bits. Assume that we want to hide five bits of data in each fragmented patches of 8x8, and then divide the secret information bits into a group of five bits.

iv) Find the decimal equivalent of those five bits. Suppose bits are 1110, its value in decimal is 30. The elements of 30th row of public key encryption table are XORed with first block pixel values. Index of the row represents the secret information bits. Since XOR operation is reversible, at the decoder side, by XOR ing the marked image block contents with corresponding key, we can retrieve back the cover image contents in a lossless fashion and the binary equivalent of index of the key represents the secret information bits. It results in joint decoding of cover medium information as well as payload information.

Figure 3.1 describes block diagram of encoder.

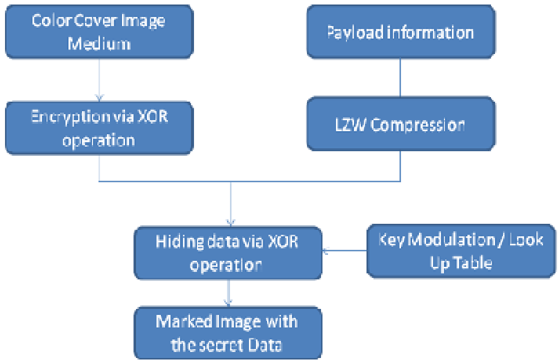

Color Cover Image Medium
Payload information
Encryption via XOR operation
LZW Compression
Hiding data via XOR operation
Key Modulation / Look Up Table
Marked Image with the secret Data

Fig. 3.1: Block Diagram of Encoder.

Step 5: First Level decryption of marked image: As a First level of decryption, the marked image with secret information embedded is XOR ed with same stream cipher key used for encoding the cover medium information contents at the encoder side.

Step 6: Joint decryption of payload information and cover medium information bits: First level decrypted cipher image is fragmented into same block sizes as done at the encoder side. These fragmented blocks are indexed and fed as an input to image classifiers for classifying them as encrypted and non encrypted image patches. Classification is made based on trained features of support vectors. In the proposed algorithm, we use two of the most powerful classifiers SVM and KNN. The output of the classifier is a matrix as shown below. To differentiate encrypted and original unencrypted image blocks, a feature vector

F = (E, H, σ, v1, v2, v3, v4) is designed by integrating the characteristics from multiple perspectives.

X	1	2	3	4	5	-	-	64
1	1	1	0	1	1			1
2	1	1	1	1	1			1
3	1	0	1	1	1			1
4	1	1	1	1	1			1
5	1	1	1	0	1			1
6	1	1	1	1	1			0
7	1	1	1	1	0			1
8	0	1	1	1	1			1

Is decoded as

Q8	Q3	Q1	Q5	Q7	
			Q6		
					Q6

Fig. 3.2: Output of Image Classifiers Considering Number of Secret information Bits Hidden in Each Block =3 and Block Size =8x8.

Figure 3.2 describes how image classifiers classify the image patches into 2 classes one and zero and their corresponding index which represents the secret information.

If a particular block of a marked image is classified as encrypted block, knowing the decryption public key we can retrieve both the payload information and cover medium information. Hence joint extraction of error free cover and payload information is possible by XOR ing the marked image block contents with the corresponding indexed row of public key encryption table. Similarly decode each block of the marked image to reconstruct carrier.

Step 7: Decompression of secret information bits using LZW Decompression technique: At this stage, the recovered sensitive data is in reduced form. It is decoded by Using LZW decompression technique.

Step 8: Evaluation of effectiveness of proposed algorithm: As a final step, the efficiency of the proposed algorithm is verified through various evaluation parameters like embedding capability, accuracy in comparison with existing techniques

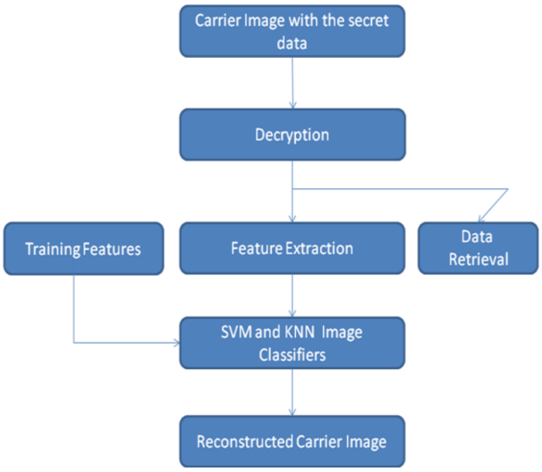
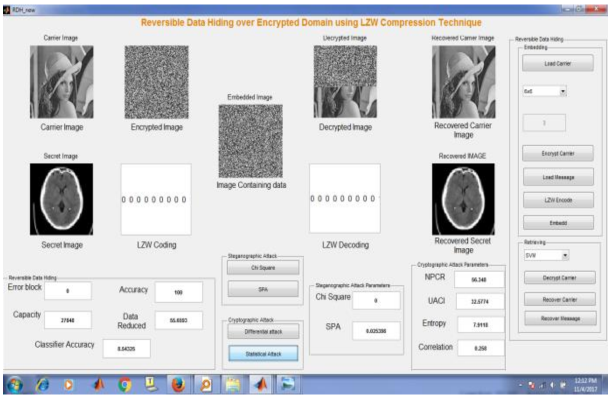

Carrier Image with the secret data
Decryption
Training Features
Feature Extraction
Data Retrieval
SVM and KNN Image Classifiers
Reconstructed Carrier Image

Fig. 3.3: Describes Decoding Process and Joint Extraction of Host and Payload Image Information.

4. Results and discussion

In this section, sufficient evaluated results are listed to provide the proof of efficiency of proposed algorithm by considering various color and grey scale test images. The effectiveness of the proposed algorithm is evaluated through parameters like peak signal to noise ratio, embedding capacity and the amount of data reduced by using LZW compression technique.

Effectiveness of two of the image classifiers SVM and KNN classifiers are compared in terms of their ability to correctly categorize the image blocks into encrypted and non encrypted blocks. The effectiveness of the algorithm is also evaluated in terms of its ability to prove resistant to various cryptographic and steganographic attacks.



0 0 0 0 0 0 0 0 0

5x5

1

SVM

Error block 0

Accuracy 100

Capacity 27848

Data Reduced 55.6893

Classifier Accuracy 8.54326

Chi Square 0

SPA 0.025398

NPCR 66.348

UACI 32.5774

Entropy 7.9118

Correlation 0.258

Fig. 4.1: GUI Considering DICOM Image as the Secret Information to Be Embedded.

From the above Figure 4.1, it is clearly proven that the proposed technique is proven more resistant to various steganographic and cryptographic attacks. Amount of secret information embedded is around 27,488 bits with hundred percent error free retrieval of both host image signal as well as secret image information. SVM Image classifier accuracy is 8.54, almost nearing to ideal value. Figure 4.2 shows sample test images of size 512x512, considered to prove the effectiveness of the proposed algorithm.

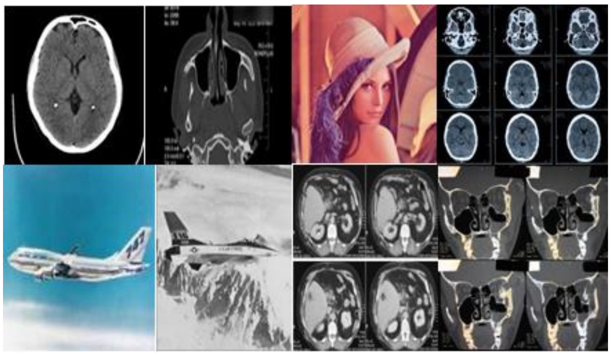
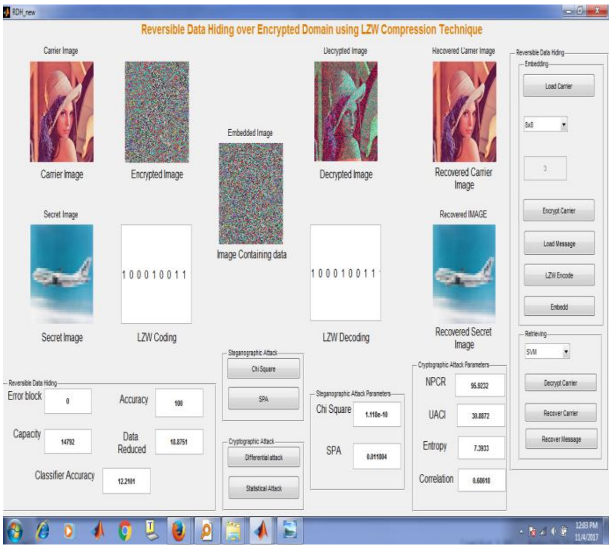


Fig. 4.2: Sample Test Images.

Figure 4.3 and 4.4 describes graphical user interface considering color image as the host and payload information considering both SVM and KNN classifier.



1 0 0 0 1 0 0 1 1

8x8

3

SVM

Error block 0

Accuracy 100

Capacity 14792

Data Reduced 18.8751

Classifier Accuracy 12.2101

Chi Square 1.118e-10

SPA 0.011804

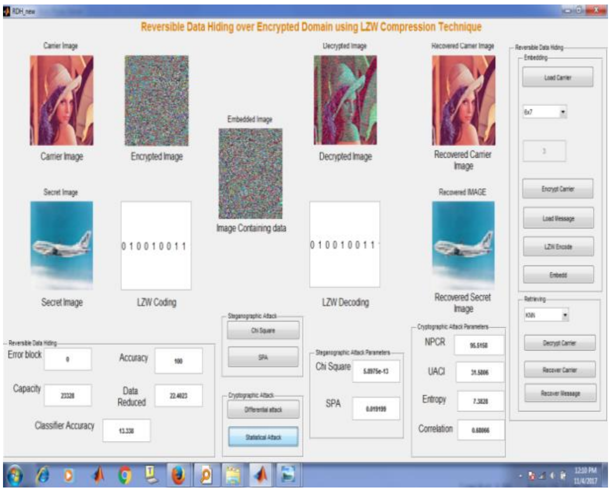
NPCR 95.9232

UACI 30.8872

Entropy 7.3933

Correlation 0.68618

Fig. 4.3: GUI Considering Color Image as Host and Payload Information with SVM Classifier.



0 1 0 0 1 0 0 1 1

6x7

3

KNN

Error block 0

Accuracy 100

Capacity 23328

Data Reduced 22.4023

Classifier Accuracy 13.338

Chi Square 5.8975e-13

SPA 0.019199

NPCR 95.5158

UACI 31.5806

Entropy 7.3828

Correlation 0.68066

Fig. 4.4: GUI Considering Color Image as Host and Payload Information with KNN Classifier.

Table 4.1: Comparison between Huffman and LZW Coding Technique in Terms of Amount of Data Reduced In Percentage

Block Size	Data Reduced in % using Huffman Coding	Data Reduced in % using LZW Coding
8X8	11.682	16.928
7X7	11.8606	20.065
6X7	11.5917	20.203
6X6	11.5124	22.166
6X5	11.5417	25.363
5X5	11.4685	28.930

From the above table 4.1, it is proved that compression ratio considering various block size is more using LZW compression technique in comparison with Huffman coding. Hence proposed technique results with greater embedding capacity.

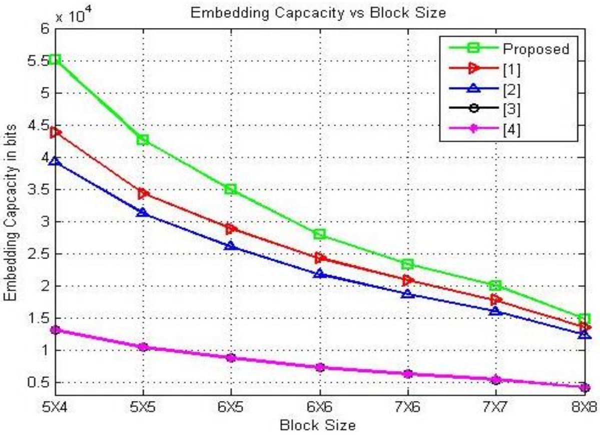


Fig. 4.5: Embedding Capacity versus Block Size.

Figure 4.5 shows plot of data hiding capability versus block size. It clearly proved from the plot that as the block size increases Embedding capacity reduces. The Proposed technique results with higher embedding capacity in comparison with reference [1], [2] and [4].

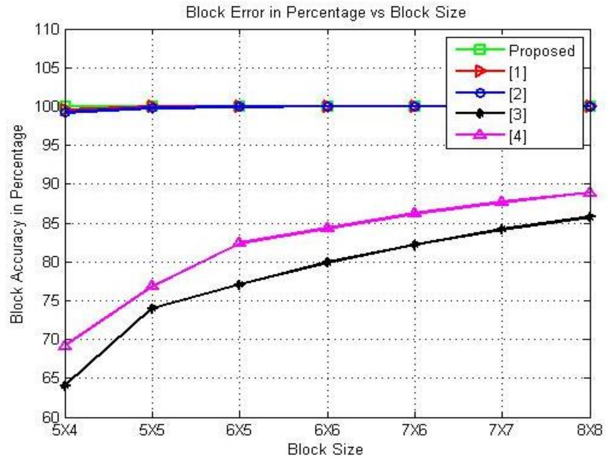


Fig. 4.6: Block Accuracy in Percentage versus Block Size.

Figure 4.6 shows block accuracy in percentage versus block size in comparison with reference [1], [2], [3] and [4]. It is clearly shown from the plot that proposed technique is hundred percent accurate for any block size in comparison with existing techniques.

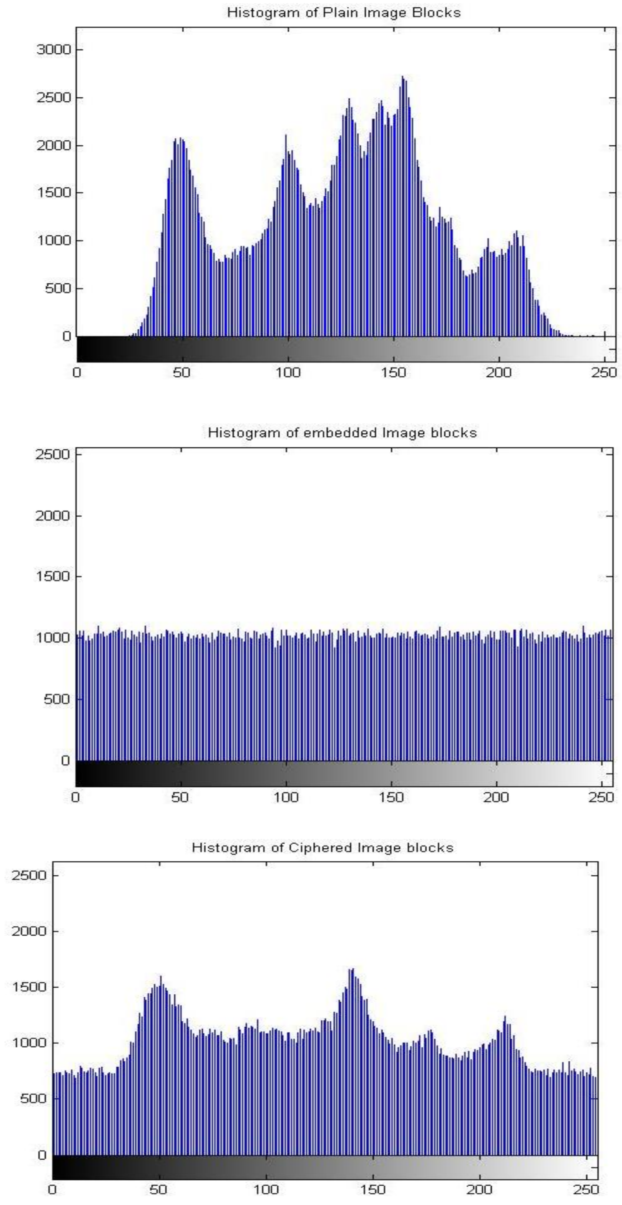


Fig. 4.7: Histogram Plots of Plain, Ciphered and Embedded Images.

Figure 4.7 shows histogram plots of plain, encrypted and marked images. It is clearly shown from the plot that histogram of embedded image is uniform in comparison with plain and ciphered images. Hence it is used as one of the training parameters for classification.

Table 4.2: A): Capacity and Accuracy of Proposed Technique in Comparison with Huffman Compression

Proposed Algorithm			Huffman Encoding	
Block Size	Capacity	Accuracy	Capacity	Accuracy
8X8	14792	100%	13448	100%
7X7	20000	100%	17672	100%
7X6	23328	100%	20808	100%
6X6	27848	100%	24200	100%
6X5	34848	100%	28800	100%
5X5	42632	100%	34320	100%
5X4	55112	99.9923%	43808	99.9923%

Table 4.2: B) Capacity and Accuracy of Proposed Method in Comparison with Ref [1], [2] and [3]

Ref [1]		Ref [2]		Ref [3]	
Capacity	Accuracy	Capacity (%)	Accuracy	Capacity (%)	Accuracy
12288	100	4096	89.44	4096	92.04
15987	100	5329	87.20	5329	90.65
18615	100	6205	85.74	6205	89.69
21675	100	7225	84.19	7225	88.88
26010	99.99	8670	82.16	8670	87.63
31212	99.99	10404	79.93	10404	86.19
39168	99.99	13056	77.10	13056	84.32

Table 4.3: Chi Square Attack Comparison

Block Size	Proposed LZW	Huffman	[4]	[5]
8X8	1.1102e-16	$5.5511x10^{-16}$	$5\ x10^{-15}$	1
7X7	1.8985e-14	$1.0669x10^{-13}$	$1.0x10^{-15}$	$1.0x10^{-14}$
7X6	1.1102e-16	$4.019x10^{-14}$	$1x10^{-14}$	$1x10^{-10}$
6X6	6.7724e-15	0	$1x10^{-16}$	$1x10^{-13}$
6X5	1.5543e-13	$7.7716x10^{-16}$	$5x10^{-14}$	$5x10^{-12}$
5X5	0	$2.8866x10^{-15}$	$1x10^{-14}$	$1x10^{-14}$
5X4	6.6613e-16	$2.7756x10^{-15}$	$1x10^{-14}$	$1x10^{-13}$

Above table 4.3 proves that proposed technique is more resistant to chi square attack in comparison with existing techniques. Hence algorithm is proven more secured. Ideal value is nearer to zero for the algorithm to be more secured.

Table 4.4: Classifiers Accuracy Comparison Considering Various Block Sizes

Block Size	Classifier Error SVM	Classifier Error KNN
8X8	12.182617	12.185669
7X7	12.300619	12.286345
6X7	13.894037	13.956487
6X6	12.773857	12.465398
6X5	19.512687	17.301038
5X5	24.953143	21.968714
5x4	29.276769	23.161765

From the table 4.4, it is clearly observed that KNN classifier has less error in classifying image patches into two classes in comparison with SVM classifier.

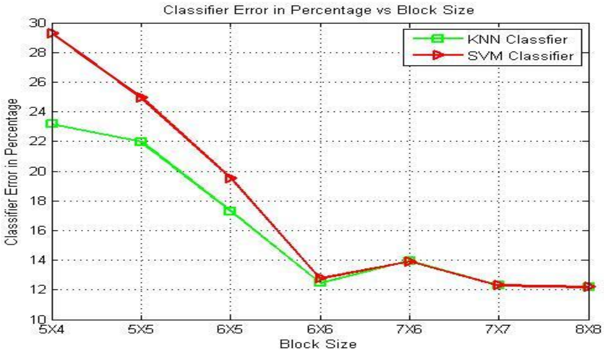


Fig. 4.8: Error Comparison with Different Classifiers.

Figure 4.8 shows a plot of error percentage. It is less with KNN classifier in comparison with SVM classifier.

Table 4.5: Feature Values of Encrypted Blocks

V1	σ	H	E	V2	V3	V4
0.7481	0.1385	0.0133	0.2500	0.8181	0.7516	0.6986
0.7650	0.1364	0.0120	0.2500	0.7241	0.5805	0.5997
0.7884	0.1309	0	0.2188	0.6841	0.5903	0.6591
0.0066	0	0	1.2813	0.0167	0.0156	0.0156

Table 4.6: Feature Values of Non Encrypted Blocks

	σ	H
0.881	0.1388	0
0.756	0.1389	0.0142
0.936	0.1388	0.0138
0.829	0.1380	0

E	V2	V3	V4
0.1875	0.7541	0.8364	0.6317
0.1875	0.8255	0.7416	0.6389
0.1875	0.7723	0.8159	0.6206
0.2188	0.8194	0.8284	0.6058

Table 4.5 and 4.6 shows the feature values of encrypted and non encrypted image blocks used for classification.

5. Conclusion

The Proposed algorithm is a high performance, a high embedding and novel secured reversible data hiding technique using different types of host images, considering image data as secret information. LZW compression algorithm is used to compress the secret sensitive information, which results in high embedding capacity. Signal processing is done over encrypted host image to protect confidentiality of host image. Effective two class off line trained SVM classifier and K-NN classifier is made use at the receiver end to categorize ciphered and non ciphered picture patches. Categorization is based on feature values which are seven in number, summing the features from multiple angles. Sufficient experimental proofs are listed to provide proof for the novelty and efficiency of the proposed technique. Experimentally proven results prove that suggested technique provides higher embedding capacity and error free reversible data embedding method. The proposed method is proven highly resistant considering steganographic and cryptographic attacks.

References

[1] Jiantao Zho, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation". IEEE Transactions on Circuits and Systems for Video Technology PP.441 – 452, 2016.

[2] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[3] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.* vol. 19, no. 4, pp. 199–202, Apr. 2012.

[4] Soria-Lorente and S. Berres, "A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information" Security and Communication Networks Volume 2017 (2017), Article ID 5397082.

[5] L. Velasco-Bautista, J. C. L´opez-Hern´andez, M. Nakano-Miyatake, and H. M. P´erez-Meana, "Steganography in a digital image in the DCT domain.

[6] Mehmet Utku Celik, Gaurav Sharma, A. Murat Tekalp, "Lossless Generalized-LSB Data Embedding", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 14, NO. 2, FEBRUARY 2005.

[7] Mehmet Utku Celik, Gaurav Sharma, A. Murat Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an implementation", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 4, APRIL 2006.

[8] W. Puech, M. Chaumont, and O. Strauss, "A Reversible data hiding method for encrypted images" *Proc. SPIE*, vol. 6819, pp. 1–9, Feb. 2008.

[9] Yongjian Hu, Heung-Kyu Lee, and Jianwei Li, "DE-Based Reversible Data Hiding With Improved Overflow Location Map", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 2, FEBRUARY 2009.

[10] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[11] Xinpeng Zhang, "Reversible Data Hiding With Optimal Value Transfer", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 2, FEBRUARY 2013.

[12] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang , "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013.

[13] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[14] Z. Qian, X. Zhang, and S. Wang, "Reversible data hiding in encrypted JPEG bit stream," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1486–1491, Aug. 2014.

[15] Anitha Devi M.D and K. B. Shivakumar"Protection of Confidential Color Image Information Based on Reversible Data Hiding Technique (PCCIRT) IEEE International Conference on computing and Network communications (CoCoNet'15), Dec 2015 978-1-4673-7308-1/15 pp 742-747.

[16] Anitha Devi M.D and K.B.Shivakumar "A Novel Secured Reversible Covert Communication over Encrypted Domain Using SVM Classifier" IEEE explorer, september, 2017 https://doi.org/10.1109/ICACCI.2017.8126147.

[17] Yue Wu, *Student Member, IEEE*, Joseph P. Noonan, *Life Member, IEEE*, and Sos Agaian, *Senior Member, IEEE*"NPCR and UACI Randomness Tests for Image Encryption"CYBER JOURNALS: MULTIDISCIPLINARY JOURNALS IN SCIENCE AND TECHNOLOGY, JOURNAL OF SELECTED AREAS IN TELECOMMUNICATIONS (JSAT), APRIL EDITION, 2011.

[18] Sorina Dumitrescu, Xiaolin Wu and Zhe Wang "Detection of LSB Steganography via Sample Pair Analysis "IEEE explorer, 2003.

[19] John Babu, Sridevi Rangu, Pradyusha Manogna " A Survey on different feature extraction and classification techniques used in image steganalysis " Journal of Information security, 2017,8,186-202 ISSN online:2153-1242.

[20] Brindha Murugan , Ammasai Gounden Nanjappa Gounder "Image encryption scheme based on blockbased confusion and multiple levels of Diffusion IET Journals"ISSN 1751-9632 https://doi.org/10.1049/iet-cvi.2015.0344.

[21] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE TransImage Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[22] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inf.Forensics Security*, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[23] Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.

[24] B. Yang, C. Busch, and X. Niu, "Joint reversible data hiding and image encryption," *Proc. SPIE*, vol. 7541, pp. 1–10, Jan. 2010.

[25] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3976–3987, Oct. 2005.

[26] M. Barni, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 452–468, Jun. 2011.