Texture Based Video Steganography Technique Using Block-Wise Encryption

Abdul Rub
Research Scholar
Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, Uttar Pradesh
abdulrub88@gmail.com

Er. Anchit Sajal Dhar
Assistant Professor
Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, Uttar Pradesh
anchit.dhar@shiats.edu.in

Er. Mohit Paul
Assistant Professor
Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, Uttar Pradesh
mohit.paul@shiats.edu.in

***Abstract*—**

The video stenography is the technique which can hide the sensitive text data. In the past times, various techniques has been proposed for video stenography which are broadly into wavelet transformation and discrete transformation, In this research paper, novel technique has been proposed which is based on textual feature extraction, selection and encryption. The GLCM algorithm is applied for the textual feature analysis, PCA algorithm is used for feature selection and block wise encryption is applied to generate final stegno image. The proposed algorithm is implemented in MATLAB and it has been analyzed that it performs well in terms of PSNR and MSE.

Keywords- GLCM, PCA, Block wise encryption, PSNR, MSE

i. INTRODUCTION

In order to hide the data from external users, there are various modifications made for which the steganography and cryptography techniques are used the most these days. There are large numbers of applications which include the usage of these techniques. They help in hiding the messages, the secret information related to credit cards and for various such applications.

The conversion of important information into unreadable form is known as encryption. Encryption is utilized as a secure mechanism in order to protect the data from past few decades by various organizations and single users. With the increase in growth of digital world there has been an increase in demand of securing the digital images. The block diagram of encryption and decryption process is shown below in figure 1, which an image is converted into ciphered object. A cipher key is applied to the image for protecting it [2].

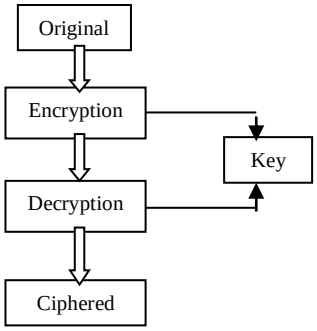

Figure 1: General Block Diagram of Encryption/Decryption Process

There are numerous properties present within an image. An image that contains all the objects distinguished from each other is known as an image with good and clear features. In order to handle the subset of features of an image there are mainly two different ways. They are feature extraction and feature selection. In order to extract the most important data from raw object, the feature extraction process is applied. This process helps in identifying the set of parameter which can define the shape of a character in a proper manner. The set of features is extracted which helps in increasing the recognition rate. It utilizes minimum number of elements in it. Further the comparative feature set is created for assorting the similar symbol within the process. In order to select a subset of input variables the feature selection process is used. The features are chosen here on the basis of very less or almost no predictive information. This helps in increasing the accuracy of classification process [3].

The initial phase executed in the work proposed in this paper is the pre-processing phase. Here, two random video frames are chosen as input images. One of these images is utilized for creating a key and the other image is used for providing encryption with that key used. Further, with the help of gray level co-occurrence matrix algorithm the various texture features of an image are extracted. The principal component analysis algorithm is

applied in order to choose the best features. Further, the second image is partitioned into numerous blocks. Each block here is encrypted by applying chaos-based image cryptosystem in it.

The further sections of this paper are summarized as follows: The past work related to this research is presented in Section 2. Section 3 explains the proposed methodology along with the flowchart. The various experimental results are presented in Section 4 along with the analysis made. The conclusion of the proposed work is summarized at the last section which is Section 5.

ii. RELATED WORK

In 2011, Guoji Zhang et al, proposed in this paper a novel image encryption method which helps in defining the skew tent chaotic map. This method further helps in generating permutation-diffusion architecture within this paper. The P-box is chosen as a similar size of plain image within this method. This helps in changing the location of pixels. The plain-image helps in identifying the key stream which is generated by the skew tent chaotic map. In order to provide reliable network security and secure communications within the networks, this method is highly beneficial. The attacks possible in the network can be prevented with the help of key space. It is seen through the statistical analysis that the image can be protected from any kinds of statistical attacks occurring within the network with the application of proposed method [4].

In 2014, Shabir A. Parah et al. proposed in this paper a data hiding mechanism which will include within it the scrambling and pseudorandom methods. This helps in providing a two layer security to the embedded data. A good perceptual transparency can be seen on the stego images generated through this mechanism [5].

In 2015, Wen Chen et al. proposed in this paper a new method in order to provide encryption to multiple-image encryption. The three-dimensional space is utilized here within which a series of particle-like points are appropriated. This is mainly done with the help of isolation of each of the information present in the image. The encryption of all the particle-like points is done into phase-just mask through this method. As per the simulation results achieved it can be seen that the proposed method enhances the security within the 3D applications as well [6].

In 2016, Venkata Krishna et al. proposed in this paper a new image encryption mechanism that includes the AES and visual cryptography methods. The main motive here is to protect the image for which an encoding mapping is proposed. This method helps in converting the key into shared with respect to the Visual Secret Sharing mechanism. By making modifications in the key shares the confidentiality is tested here. This is to be done before the data arrives towards the destination. As per the simulation results it is seen that in case there are any encrypted shares attained by the intruder from the network, the original secret image cannot be accessed without the application of cipher on it. This results in keeping the data still secure [7].

In 2016, Xianye Li et al. proposed in this paper a new multiple-image encryption mechanism. The modified logistic map algorithm is included along with the coordinating sampling and compressive ghost imaging in order to secure the data. This results in increasing the feasibility of the method. Initially, the random phase-just masks are generated along with the application of modified logistic map algorithm. Further, the next step focuses on creating 2Ddiscrete cosine transformation (DCT) operation from the multiple secret images. The random sequences observed here are scrambled which are further grouped to an image. The sampling matrices are utilized in order to group these images amongst which the consolidated image is placed in the object place of the used method [8].

In 2016, Malika Sharma et al. proposed in this paper an image encryption method which includes the two stage iterative logistic map in it. In order to extract an image in single output, an image encryption method is to be generated. This results in including legitimate level of confusion and diffusion within the system. It is seen through the experimental results that the proposed method provides more secure mechanism which helps in improving the performance of this method in comparison to the other methods [9].

iii. THE PROPOSED METHOD

This work is based on image encryption and basepaper technique is applied on enciphering application in which image is transmitted unsecured channels. To encrypt the image for the transmission over un secured channels image is divided into blocks. The image when divided into blocks and these divided blocks are rearranged to encrypt the image. The blocks are shuffled into fixed pattern and this pattern is decided by the key which used for encryption. The key is derived based on relationship between pixels of the image. The proposed technique performs well and it is been analyzed that proposed technique provide good results against various attacks. In future, we will work on key generation phase to drive key based on textural features of the image so that pixel loss

will be minimum at the time of decryption. The proposed algorithm can be applied in the following steps:-

1. Pre-processing Phase: - In the pre-processing phase, the two image are taken as input. The first image is the image which need to encrypt and second image is the image from which key need to generate.

2. Feature extracted:- In the second phase, the textual features of the first image is extracted using the glcm algorithm. The glcm algorithm will extract the features like energy, entropy etc. image.

GLCM algorithm

1. Count all the number of pixels in the matrix in which the data is saved.

2. Store the counted pixels in matrix P[I,j].

3. Check similarity between pixels in the matrix by applying histogram technique.

4. Calculate contrast factor from the matrix:

$$g = \exp[\frac{mean(I) - minimum(I)}{maximum(I) - mean(I)}]$$

5. The elements of g need to be normalized by dividing the pixels.

$$g = \begin{bmatrix} 0.8\ if\ g < 0.8 \\ 1.2\ if\ g > 1.2 \\ g\ otherwise \end{bmatrix}$$

3. **Apply PCA algorithm** :- In the third phase, the PCA algorithm is applied which will select the extracted features from the first image. Linear Discriminant Analysis (LDA), Independent Component Analysis and PCA are a portion of the techniques utilized for feature extraction, among them PCA is intense method in image formation, Data examples, similarities and differences between them are identified effectively. The other principle advantage of PCA is dimension will be reduced by maintaining a strategic distance from redundant information, without much loss. Better comprehension of principal component analysis is through statistics and a portion of the mathematical techniques which are Eigen esteems, Eigen vectors. PCA is a valuable statistical and common method that has discovered application in fields, for example, image recognition and compression. Principal Component Analysis (PCA) is a mathematical methodology that utilizations linear Transformations to map data from high dimensional space to low dimensional space. The low dimensional space can be controlled by Eigen vectors of the covariance matrix.

The steps involved in PCA include:

• The mean valve S of the given data set "S" is found

• Subtract the mean value say from S. from these valves a new matrix is obtained. Let say "A"

• Covariance is obtained from the matrix i.e., C = AAT Eigen values are obtained from the covariance matrixes that are V1V2V3V4…VN,

• Finally Eigen vectors are calculated for covariance matrix C

• Any vector S or $S - \bar{S}$ or can be written as linear combination of eigen vectors shown in Equation below.

• Because covariance matrix is symmetric it form basis $V_1V_2V_3V_4 \ldots V_N$,

$$V_N S - \bar{S} = b_1u_1 + b_2u_2 + b_3u_3 + \cdots + b_Nu_N$$

• Only Largest eigen values are kept to form lower dimension data set:

$$\hat{S} - \bar{S} = \sum_{I=0}^{1} b_1u_1 ; 1 < N$$

The components in lower dimension space are called principal components which are ensured to be independent just if the data set is mutually typically appropriated. PCA is delicate to the relative scaling of the original variables. Contingent upon the field of application, it is additionally named as discrete Karhunen-Loève Transform (KLT), or the Hotelling transform.

4. **Encryption of second image** :- In the next step, the keys are generated from the second image. The first image is divided into blocks and each block is encrypted individually to generate final encrypted image. The chaos-based image cryptosystem fundamentally consists of two stages. The plain image is given at its input. There are two stages in the chaos-based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the whole image

without exasperating the value of the pixels and the image ends up plainly unrecognizable. The pixel permutation is completed by a chaotic system. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of every pixel in the entire image a vital tool to shield image from attackers.

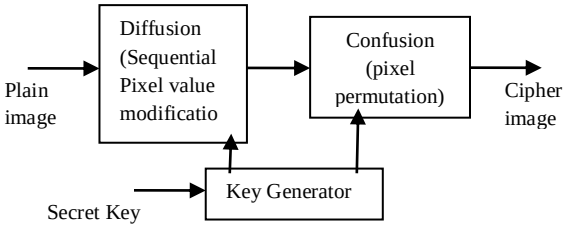

Figure 1. Architecture of Chaos-based image cryptosystem

The confusion stage is the pixel permutation where the position of the pixels is scattered over the whole image without disturbing the value of the pixels and the image ends up noticeably unrecognizable. In this way these initial conditions and control parameters fill in as the secret key. It is not exceptionally secure to have just the permutation stage since it might be broken by any assault. To improve the security, the second stage of the encryption process aims at changing the value of every pixel in the entire image.

The process of diffusion is likewise brought out through a chaotic map which is for the most part dependent on the initial conditions and control parameters. In the diffusion stage, the pixel values are modified sequentially by the sequence produced from one of the three chaotic systems chosen by outside key. The entire confusion-diffusion round repeats for various times to accomplish an agreeable level of security. The haphazardness property characteristic in chaotic maps makes it more reasonable for image encryption.

iv. EXPERIMENTAL RESULTS AND DI SCUSSION

The proposed algorithm is the image stenography algorithm which is based on the glcm for the feature analysis, PCA algorithm for feature selection and chaos based image encryption. The proposed algorithm is implemented in MATLAB and results are analyzed in the form of MSE and PSNR

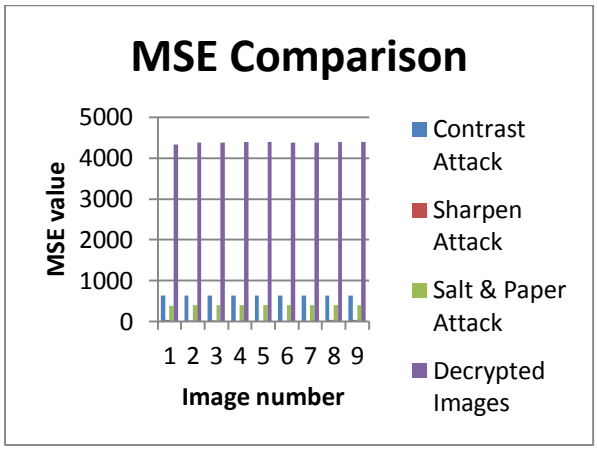

Fig 2: MSE Comparison

As shown in figure 2, the MSE value of various scenarios like salt & pepper, contract, sharpen and decryption is compared and it has been analyzed that proposed algorithm has least impact of the attacks

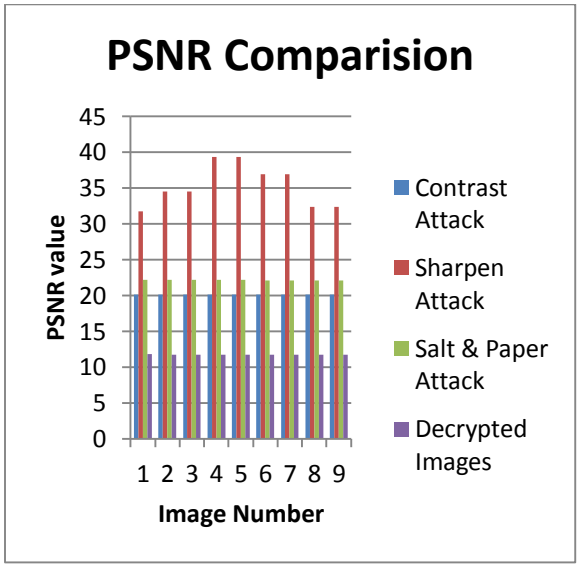

Fig 3: PSNR Comparison

As shown in figure 3, the PSNR values of the contrast, sharpen, salt & pepper and decryption is compared and it has been analyzed that sharpen is the attack which has minimum impact on the proposed algorithm

I. *CONCLUSION*

In this work, it has been concluded that video stenography is the efficient technique to provide security to the sensitive data. The general image stenography techniques are classified into wavelet based and discrete techniques. In the work, novel technique has been proposed which is based on feature extraction, selection and generation of stegno image. The performance of proposed algorithm is

tested in terms of MSE and PSNR. It has been analyzed proposed algorithm well in terms of these two parameters

REFERENCES

[1] Ramadhan J. Mstafa and Khaled M. Elleithy, "A highly secure video steganography using hamming code (7, 4)", 2014.

[2] S. Rohith, K. N. H. Bhat and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register", 2014, International Conference on Advances in Electronics, Computers and Communications (ICAECC).

[3] S. Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)", 2014, International Conference on Contemporary Computing and Informatics (IC3I).

[4] Guoji Zhang, Qing Liu, "A novel image encryption method based on total shuffling scheme", 2011, Optics Communications 284 2775–2780.

[5] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz, G.M. Bhat, "Data hiding in scrambled images: A new double layer security data hiding technique", 2014, Computers and Electrical Engineering 40 pp.70–82.

[6] Wen Chen, "Optical Multiple-Image Encryption Using Three-Dimensional Space", 2015, IEEE.

[7] Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan, "A Novel Image Encryption Algorithm using AES and Visual Cryptography", 2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016).

[8] Xianye Li, Xiangfeng Meng, Xiulun Yang, Yongkai Yin, Yurong Wang, Xiang Peng, Wenqi He, Guoyan Dong, Hongyi Chen, "Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling", 2016, IEEE.

[9] Malika Sharma, Anuja Bhargava, "Chaos Based Image Encryption Using Two Step Iterated Logistic Map", 2016, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE).

[10] M. P. Priyanka, E. Lakshmi Prasad, Dr. A. R. Reddy, "Fpga Implementation of Image Encryption And Decryption Using AES 128-Bit Core", 2016, IEEE.

[11] Arul Thileeban S, "Encryption of images using XOR Cipher", 2016, IEEE.

[12] Huiqing Huang, Shouzhi Yang, "Color image encryption based on logistic mapping and double random-phase encoding", 2017, IET Image Process., Vol. 11 Iss. 4, pp. 211-216.

[13] Zaheer Abbas Balouch, Muhammad Imran Aslam, Irfan Ahmed, "Energy Efficient Image Encryption Algorithm", 2017, IEEE.

[14] Haralick, RM., K. Shanmugan, and I. Dinstein, Textural Features for Image Classification, IEEE Transactions on Systems , Man, and Cybernetics, Vol. SMC-3, 1973, pp. 610-621.

[15] Taneja, N., Raman, B., Gupta, I., "Selective image encryption in fractional wavelet domain", 2011, Int. J. Electron. Commun., 65, pp. 338–344.