

# Secure Image Transmission and Evaluation of Image Encryption

Reshu Choudhary<sup>1</sup> and Arun JB<sup>2</sup>

<sup>1</sup> Research Scholar, Bhagwant University,  
Ajmer, Rajasthan, India

<sup>2</sup> Teacher's Training center, Govt. Polytechnic Collage,  
Jodhpur, Rajasthan,  
India

## Abstract

In the digital world, security is an important issue, and encryption is one of the ways to ensure security. The need to develop new encryption schemes comes from the fact that traditional encryption schemes for textual data are not suitable for multimedia data stream. Valuable multimedia content such as digital images, however, is vulnerable to unauthorized access while in storage and during transmission over a network. A new algorithm is presented for hiding a secret image in the least significant bits of a cover image. The images used may be color or grayscale images. A fundamental task in many image processing applications is the visual evaluation of a distorted image. There are many measures for examining image quality, such as the mean structural similarity, mean absolute error, Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). It is computed by averaging the squared intensity differences of distorted and original image pixels, along with the related quantity of the PSNR. Experimental results show that same size images are efficiently encrypted with reliable PSNR as compared with different size images. MATLAB based coding manage the query phase of the system. Based on the simulation results, the proposed system not only shows the efficiency in hiding the attributes but also provides better cover image selection.

**Keywords:** Cryptography, secure image transmission, PSNR evaluation, image encryption, features protection.

## 1. Introduction

There are many digital images are present in digital communication system which being sent over computer networks. With the increasing growth of multimedia applications like audio, video and images. Security is an important aspect in digital communication. There is one of the obvious way to ensure security is Image encryption. This technique is try to convert original image to another image which is hard to understand and to keeps the image confidential between users, in other word, it's important that without decryption key no one can access the content. Image encryption has applications in internet communication, multimedia systems, medical imaging,

telemedicine, military communication etc. For privacy protection of digital images, encrypted databases is an important technological capability in multiparty information management. There are many online services of webmail such as Gmail, photo hosting such as Flickr, and financial management such as Mint.com, where users store their private information on some remote server and the server provides functionalities to the user, such as categorization, search and data analysis [1].

Encryption of multimedia data can be the immediate solution to protect information against unauthorized access. Such type of techniques required encryption of the data through some sort of mathematical tools where only the actual party that shares the data could possible decrypt to use the data. Encryption uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important. Image hiding or encrypting method and algorithm can be very from simple methods to more complicated and reliable frequency method. Most of the encryption algorithms which are available mainly used for text data and cannot be suitable for multimedia data such as images. Measurement of image quality is important for many image processing applications [2]. Image quality assessment is closely related to image similarity assessment in which quality is based on the differences between a degraded image and the original, unmodified image. There are two ways to measure image quality by subjective or objective assessment. Subjective evaluations are expensive and time-consuming [3]. It is impossible to implement them into automatic real-time systems. Objective evaluations are automatic and mathematical defined algorithm. Subjective measurements can be used to validate the usefulness of objective measurements. Therefore objective methods have attracted more attentions in recent years. Well-known objective evaluation algorithms for measuring image quality include Mean Squared Error (MSE), Peak Signal-

to-Noise Ratio (PSNR), and Structural Similarity (SSIM). MSE and PSNR are very simple and easy to use.

## 2. Literature Survey

With the growing development of digital communication, the communication through multimedia components is on demand. The data like text, images, video and audio is communicated through network. For security issues Cryptographic techniques are used which gives security Services like Confidentiality, Data Integrity, and Authentication to protect against the attacks. In 1996, Manezes introduced that Cryptography is the study of hiding information related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography protects information by transforming it into an unreadable format [4]. The original text, or plaintext, is converted into a coded equivalent called cipher text via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the cipher text into plain text. Yonglin Ren, Azzedine Boukerche [5], Lynda Mokdad presents the principle of selective encryption with propose of probabilistically selective encryption algorithm. The algorithm was based on symmetric key [6-7]. S. Kala implemented the idea of selective encryption algorithm for wireless ad hoc network with the Quadrature Mirror Filters and Lossless compression techniques.

### 2.1 Image Encryption Techniques:

As per increase in usage of digital techniques for transmitting and storing images, it become important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time encrypt the images to make images more secure. In 2007. M. Zeghid introduces Modified-AES technique in which block and key lengths are 128 bits and 128, 192 or 256 bits. In this technique encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. To minimize high calculation we skip the Mix column step and add the permutation. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms, high calculation and computation overhead [8]. In 2008, Mohammad Ali Bani Younes and Aman Jantan proposed technique in which the original image was divided into blocks, and again rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm [9]. In modified technique

image is divided in to fixed size blocks, then blocks are transformed into new location using various permutation techniques. The results showed that the correlation between image elements was significantly decreased and higher entropy was achieved [10]. In 2008, Selin Aviyente proposed a new Least Square Approximation based technique. In this technique translation of the original image into the form of encrypted one by the randomly generating vectors and decrypted by using LSA concept [11].

In 2009, Bibhudendra Acharya proposed a advanced Hill encryption technique which uses an involuntary key matrix. It overcomes the problems of encrypting images in fast real time application. It applicable over both gray and color images. In this technique involuntary key matrix of fixed size is constructed and then plain image is divided into same size blocks [12]. In 2010, Lala Krikor proposed a technique that is based on encrypting of Discrete Cosine Transform (DCT) coefficients. It is the mathematical transformation technique which takes a signal and transforms it from spatial domain into frequency domain. JPEG and MPEG format uses this technique to concentrate image information by removing spatial data redundancies in two-dimensional images [13]. Again in 2010, Panduranga H.T and Naveen Kumar S. K propose a hybrid technique for image encryption which employs the concept of carrier image and SCAN patterns generated by SCAN methodology. The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths [14].

### 2.2 Image Evaluation Techniques:

For evaluate the performance of digital imaging systems with respect to a wide variety of distortions during acquisition, processing, storage, transmission and reproduction, any of which may result in a degradation of visual quality. Some commonly used methods to evaluate image quality are mean squared error, peak signal to noise ratio, structural similarity index matrix etc.

#### A. Mean Squared Error (MSE)

One obvious way of measuring similarity is to compute an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal [15-22]. The mean-squared-error is the simplest, and the most widely used. For good image quality its value is became low. This metric is frequently used in signal processing and is defined as follows:-

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (x(i, j) - y(i, j))^2 \quad (1)$$

Where  $x(i, j)$  represents the original (reference) image and

$y(i, j)$  represents the distorted (modified) image and  $i$  and  $j$  are the pixel position of the  $M \times N$  image. MSE is zero when  $x(i, j) = y(i, j)$ .

**B. Peak Signal to Noise Ratio (PSNR)**

The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error [15-22]. If PSNR value is high it shows good quality image.

$$PSNR = 10 \log_{10} \frac{(2^n - 1)^2}{\sqrt{MSE}} \quad (2)$$

In image cryptography most of the available encryption algorithms are mainly uses different size images so they readily encrypted the image. For sending small secret image they use large image size so it put dispensable burden on transmission network and require more processing at every stage. To overcome this problem proposed method is applied on color images of same size and type.

**3. Proposed Approach and Methodology**

The encrypted image produced by distinct algorithms leave some sign of encryption like visual presentation and some mathematical testing methods such as histogram evaluation, entropy, correlation etc., also provides information about encryption of image. These type of images are easily identified by hackers or unauthorized person and they can modified, resize or compress them easily. The proposed method as shown in Fig.1 gives very simple and efficient technique for hiding two same size color images. The decryption of image is only possible when cover image is available to sender and desired receiver. The cover image work as a big encryption key. The encrypted image is not identified by hackers and not by any mathematical tool.

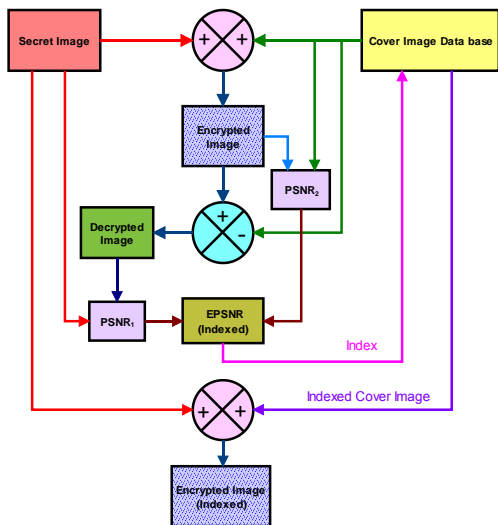


Fig.1 Proposed method for image encryption

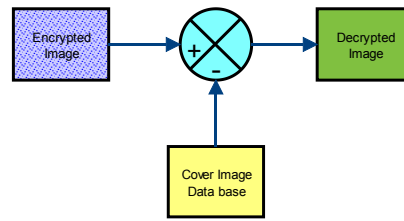


Fig.2 Proposed method for image decryption

$PSNR_1$  is noise ratio between the secret image and decrypted image. It represents the reproduced quality of the image. It so high in nature and indicate the quality of image but it reduces the visual effect on the encrypted image. So quality of encryption is not so good.

$PSNR_2$  is noise ratio between the cover image and the encrypted image. It is low in nature and indicates that the encryption is good for cover image but the decryption is poor in nature for secret image.

There is a direct relation between  $PSNR_1$  and  $PSNR_2$  both are govern by each other if  $PSNR_1$  is maximum value. Then the  $PSNR_2$  is minimum value, so there is a need of balance between both  $PSNR$ 's. That is achieved by Equal PSNR (EPSNR). EPSNR is a point where both  $PSNR_1$  and  $PSNR_2$  are nearly equal, so the advantage of both features as encryption and decryption of images are taken place.

**3.1 Proposed Algorithm**

In this we have select parameter to be calculation, select various images and pass selected images one by one through existing and proposed mechanism to calculate results.

1. Read the secret image.
2. Read cover image database. Select cover image (PA) and encrypt it with secret image (PB).The processing step undertaken by A to convert M into its encrypted form C by:

$$C = E(PA^A, E(PB^B, M)) \quad (3)$$

Where  $E( )$  stands for encryption, the processing step undertaken by B to recover D from C are:

$$D = F(PA^B, F(PB^A, C)) \quad (4)$$

Where  $F( )$  Stands for decryption.

3. Evaluate the  $PSNR_1$  and  $PSNR_2$  for the entire cover image with secret images and stored in the indexed matrix.
4. Evaluate the EPSNR of  $PSNR_1$  and  $PSNR_2$  and find the index of cover image.
5. Encrypt the image with indexed cover image.
6. Transfer image to authorized user.
7. Decrypt secret image with the use of cover image database.
8. Display the image to user.

3.2 Results

This proposed method adding encryption to a color picture, which is the art of creating hidden images, through adding color cover image with secret color image. The proposed method is tested on the well-known data of Wang. This data base has nearly 10,000 images with different sizes and types of objects like bird, forest, flowers, mountains and nature etc. The proposed method uses only images having size of 128×96 (w×h) pixels, total number of pixels are 12288 [23]. Cover image database is consists of 280 images. It is shared between sender and receiver and all secret images are encrypted only with the cover image database. The method is applied to all the cover images and calculates the EPSNR point to select the cover image for encryption of secret image. The encrypted image is send to another user that can be decrypted it by cover image database. The encrypted key lies in the cover image itself so it can be easily decrypted by desired receiver efficiently without difficulty. The performance evaluation factors PSNR for encryption is obtained from different image are summarized in Table.1.








Secret image	PSNR <sub>1</sub>	PSNR <sub>2</sub>	EPSNR	
	48.06	15.12	19.17	18.8
	46.27	9.54	13.81	12.56
	35.63	8.06	11.96	11.86
	∞	21.02	24.43	24.86
	56.34	14.94	18.90	18.45
	∞	26.81	30.13	29.98
	37.79	7.08	11.15	12.26

Table 1: Comparison of PSNR'S for different images

This proposed method is compared with other method which is given by Abdelfatah A. Tamimi and Ayman M. Abdalla in which used secret image size was smaller than the cover image size nearly 200 times [24]. So that becomes easily encrypted. In our method cover image and secret image size is same and it efficiently encrypted. Decryption at receiver side without much degradation in image takes place.

#### 4. Conclusions

Image quality measurement plays an important role in various images processing application. A great deal of

effort has been made in recent years to develop objective image quality metrics. The best way of fast and secure transmission is by using compression and encryption of multimedia data like images. In this paper proposed method used MSE and PSNR for Image Quality evaluation. This method use same size of images to encrypt and decrypt images directly for real time applications. Involving two images (the cover and the secret) in place of only one (the cover) we are able to change the cover coefficients randomly. This paper explores technique which enable similarity comparison among encrypted image features, based on which secure content based image retrieval can be achieved. We show that the combination of signal processing and cryptographic techniques, such as random projection, unary encoding, and random permutation, helps us address the problem of secure image retrieval, which is otherwise difficult using traditional cryptography alone. The proposed approach has many applications in hiding and coding messages within standard Medias, such as images or videos. As future work, we intend to study steganalytic techniques for ISC and to extend ISC to mobile video communication.

#### References

- [1] D. Song, D. Wagner and A. Perrig, "Practical Techniques for Searches in Encrypted Data," IEEE Symp. on Research in Security and Privacy, pp. 44-55, 2000.
- [2] D. Boneh, G. Crescenzo, R. Ostrovsky and G. Persiano, "Public-key Encryption with Keyword Search," Proc. of Eurocrypt, pp. 506-522, 2004.
- [3] A. Swaminathan, Y. Mao, G-M. Su, H. Gou, A. L. Varna, S. He, M.Wu and D.W. Oard, "Confidentiality Preserving Rankordered Search," Proc. of the ACM Workshop on Storage, Security, and Survivability, pp. 7-12, Oct. 2007.
- [4] R. Datta, D. Joshi, J. Li and J. Z. Wang, "Image Retrieval: Ideas, Influences, and Trends of the new age," ACM Computing Surveys, 2008.
- [5] W. Lu, A. Swaminathan, A. L. Varna and M. Wu, "Enabling Search over Encrypted Multimedia Databases," to appear in SPIE Media Forensics and Security XI, Jan. 2009.
- [6] M. Datar, N. Immorlica, P. Indyk and V. Mirrokni, "Locality Sensitive Hashing Scheme based on p-stable Distributions," Proc. of the ACM Symp. on Computational Geometry, 2004.
- [7] S. Jeong, C. Won and R. Gray, "Image Retrieval using Color Histograms Generated by Gauss Mixture Vector Quantization," Computer Vision and Image Understanding, Vol. 94, 2004.
- [8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.
- [9] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm", IAENG, Vol 35:1, IJCS 35 1 03, February 2008.

- [10] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption," IJCSNS, Vol 3, No 4, April 2008.
- [11] Mahmood Al-khassaweneh, Selin Aviyente, "Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.
- [12] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra and Ganapati Panda "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
- [13] Lala Krikor, Sami Babaet, Thawar Arif and Zyad Shaaban "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research Vol.32, No.1, pp.47-57, 2009.
- [14] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", (IJCS) International Journal on Computer Science and Engineering, Vol. 02, pp. 297-300 No. 02, 2010, .
- [15] G.-H. Chen, C.-L. Yang and S.-L. Xie, "Gradient-based structural similarity for image quality assessment", in: Proceedings of International Conference on Image Processing, Atlanta, GA, pp. 2929–2932, 2006.
- [16] F. Wei, X. Gu and Y. Wang, "Image quality assessment using edge and contrast similarity", in: Proceedings of IEEE International Joint Conference on Neural Networks, Hong Kong, China, pp. 852–855, 2008.
- [17] G. Zhai, W. Zhang, X. Yang and Y. Xu, "Image quality assessment metrics based on multi-scale edge presentation", in: Proceedings of IEEE Workshop Signal Processing System Design and Implementation, Athens, Greece, pp. 331–336, 2005.
- [18] C.-L. Yang, W.-R. Gao and L.-M. Po, Discrete wavelet transform-based structural similarity for image quality assessment, in: Proceedings of IEEE International Conference on Image Processing, San Diego, CA, pp. 377–380, 2008.
- [19] A. Shnayderman, A. Gusev and A. M. Eskicioglu, "An SVD-based grayscale image quality measure for local and global assessment", IEEE Transaction on Image Processing 15, 422–429, 2006 .
- [20] Z. Wang, E. P. Simoncelli and A. C. Bovik, "Multiscale structural similarity for image quality assessment", in: Proceedings of IEEE Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, pp. 1398–1402, 2003.
- [21] Parameshachari B D, K M Sunjiv Soyjaudah and Chaitanyakumar M V, "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering™ (IJRTE), Volume-1, Issue-6, Jan 2013.
- [22] Parameshachari B D and Dr. K M S Soyjaudah "A New Approach to Partial Image Encryption" published at Proceedings of ICAdC, AISC 174, pp. 1005–1010, Springer India, 2013.
- [23] [www-db.stanford.edu/~wangz/image.vary.jpg.tar](http://www-db.stanford.edu/~wangz/image.vary.jpg.tar).
- [24] Abdelfatah A. Tamimi and Ayman M. Abdalla, "Hiding an Image inside another Image using Variable-Rate Steganography", published in International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013.