Image Encryption for Secure Data Transfer and Image based Cryptography

Arun JB
Teacher's Training Center
Govt. Polytechnic Collage
Jodhpur, India
arun1jb@gmail.com

Reshu Choudhary
Research scholar
Bhagwant University
Ajmer, India
reshuchoudhary21@gmail.com

***Abstract*—With rapid progress in internet and digital imaging technology there are more and more ways to easily create, publish and distributed images. A major issue for computer networks is to prevent important information from being disclosed to illegal users. Valuable multimedia content such as digital images, however, is vulnerable to unauthorized access while in storage and during transmission over a network. Resent advances in visual cryptography, including probabilistic schemes and colored image sharing techniques were introduced. Visual cryptography is a method for protecting image based secrets that has a computation-free decoding process.**

This paper focuses on image feature protection techniques which enable similarity comparison among protected features. Experimental results shows that secure image retrieval can achieve comparable retrieval performance to conventional image retrieval techniques without revealing information about image content. Thus the image retrieval process becomes simple. 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 other advantages such as: (1) fast transmission of the retrieval image to the receiver, (2) searching made easy. This work enriches the area of secure information retrieval and can find applications in secure online services for images and videos.

Keywords—Cryptography, secure image retrieval, visual cryptography, content based image retrieval, feature protection.

I. INTRODUCTION

Today web is going towards the multimedia data in which image covers the highest percentage of it. But with the ever-increasing growth of multimedia applications, security is an important aspect in communication and storage of images, and encryption is the way to ensure security. Image encryption techniques try to convert original image to another image that 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. Information retrieval from encrypted databases is an important technological capability for privacy protection in multiparty information management. Representative application scenarios include online services of webmail such as Gmail, photo hosting such as Flicker, 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]. Currently, servers operate on plaintext data, making user's private information vulnerable to attacks by untrustworthy administrators and malicious intruders. To provide secure online services, technologies that protect users' privacy without sacrificing functionalities are desirable. Image retrieval based on user assigned tags, extension to content based image retrieval (CBIR) is not straightforward. CBIR systems often rely on comparing the similarity among image features, such as color histograms, shape descriptors, or salient points, which are usually high dimensional vectors. Comparing similarity among high dimensional vectors using cryptographic primitives is challenging.

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 (or similarity) 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. In this paper we use these techniques for image quality assessment for image encryption.

II. LITERATURE SURVEY

In this era, the communication through multimedia components is on demand. The data like text, images, video and audio is communicated through network. Cryptographic techniques are used to provide the protection of data and information while transmission of data over the network. The various algorithms are available for the security Services like Confidentiality, Data Integrity, and Authentication to protect against the attacks. In 1996, Manezes introduced that

Cryptography is the study of mathematical techniques 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]. By make use of probabilistic methodology and stochastic algorithm, in the process of message encryption a sender includes proper uncertainty, so that the decryption of the cipher text is done by only entrusted receiver and other unauthorized nodes have no information of the broadcasted messages on the whole. S. Kala implemented the idea of selective encryption algorithm for wireless ad hoc network with the Quadrature Mirror Filters and Lossless compression techniques. In a Toss A coin algorithm the half of the data is encrypted and another half is unencrypted .i.e., 50% of data will be encrypted and left 50% will be unencrypted and, it is transferred as it is. It requires more bandwidth. Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks.

In 2012, Priyanka Agrawal and Manisha Rajpoot introduced Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. There are lots of cryptographic algorithms are available and most like: RS DES, AES, Chaotic System, DCT, and DWT are proposed and used for image encryption and selective image encryption. Kalpana Singh and Shefalika Ghosh Samaddar have used the selective encryption technique in RSA based on singular cubic curve for the text based documents. The authors proposed to increase the speed of encryption by using selective encryption. Selective encryption is a technique which uses subset of bit stream rather than entire bit stream. In the selective encryption used only a random of whole message plain text is encrypted rather than the whole text. They have taken the benefit of symmetric key algorithm to decrease the complexity of the operation and protect the data in a reasonable computational cost and these properties make the scheme suitable for real-time applications.

Optimizing 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. So, measurement of image quality is very important to numerous image processing applications in this domain. Any imaging system can use the quality metric to adjust itself automatically for obtaining improved quality images [8-9]. It can be used to compare and evaluate image processing systems and algorithms. This can be done by subjective testing sessions, or by objective computational metrics. The only correct method of quantifying visual image quality is through subjective evaluation [10-13]. In subjective evaluation, a number of observers are selected, tested for their visual capabilities, shown a series of test scenes and asked to score the quality of the scenes. Image quality assessment is closely related to image similarity assessment. Some commonly used methods to evaluate image quality are mean squared error, peak signal to noise ratio, structural similarity index matrix etc.

III. PROPOSED APPROACH AND METHODOLOGY

In image cryptography most of the available encryption algorithms are mainly used different size images so they get easily decrypted image at receiver. In this paper image encryption is applied on colour images of same size and type. For resultant compressed data is secured by Data Encryption Standard encryption algorithm. The schematic block diagram of this proposed approach is shown in Fig. 1.

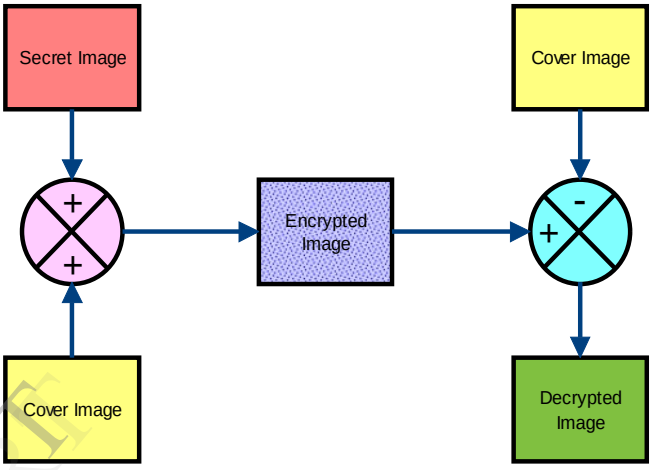

Fig.1. Block diagram of proposed method

This proposed method adding encryption to a picture, which is the art of creating hidden images, through adding cover image with secret image. This method is applied on well-known data of Wang from which 158 images are used with size of 128×96 (w×h) pixels, total number of pixels are 12288 [14]. The image database has different types of objects like bird, forest, flowers, Mountains and Nature etc.

Here are couple of test images for cryptography, encrypt secret images with cover image and to get back the original image at the receiver by decryption is applied. For evaluate image quality following methods are used:

A. Mean Squared Error (MSE)

One obvious way of measuring this 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 [15-19]. 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:-

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

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×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 [15-19]. If PSNR value is high it shows good quality image.

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

With a selected cover image the algorithm find proper secrete images from database which can be effectively encrypted. The encrypted image MSE and PSNR is used to measure the encryption quality. The lower value of MSE is shows better encryption quality and reverse is depicted by PSNR. The test results of the proposed method are shown in Fig. 2. The computation of MSE and PSNR for data set is as shown in Fig. 3 and Fig. 4 respectively.

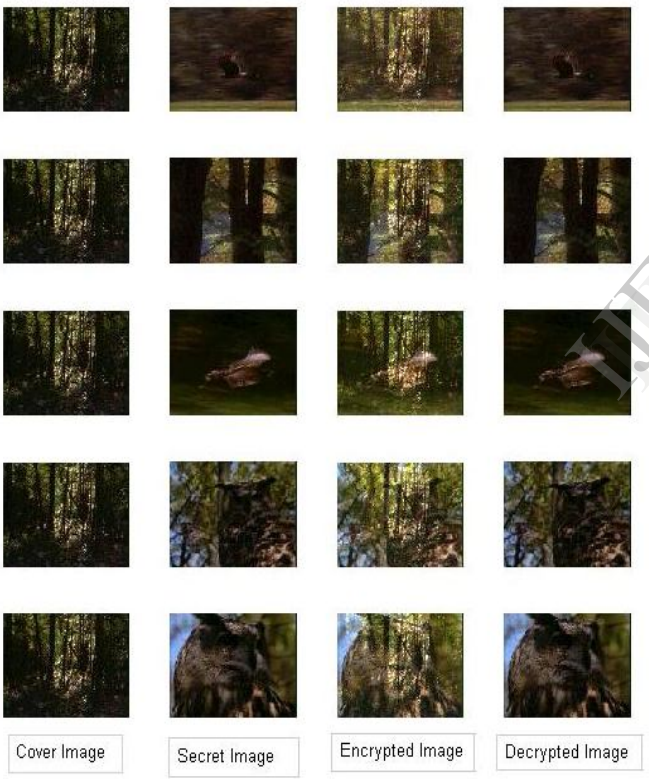

Fig.2. Test Result of Proposed Method

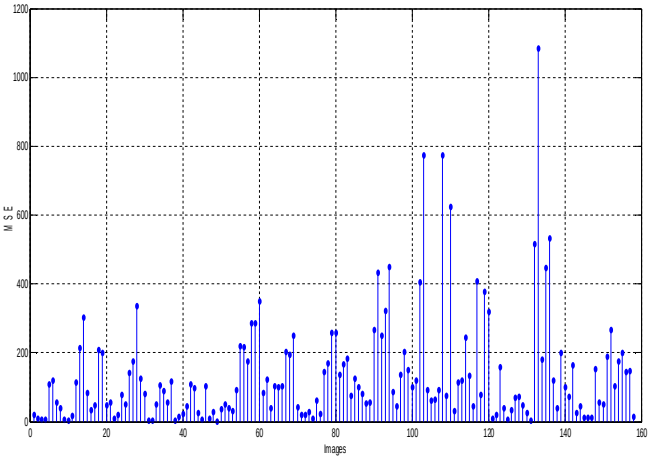

Fig.3. MSE plot for encrypted images

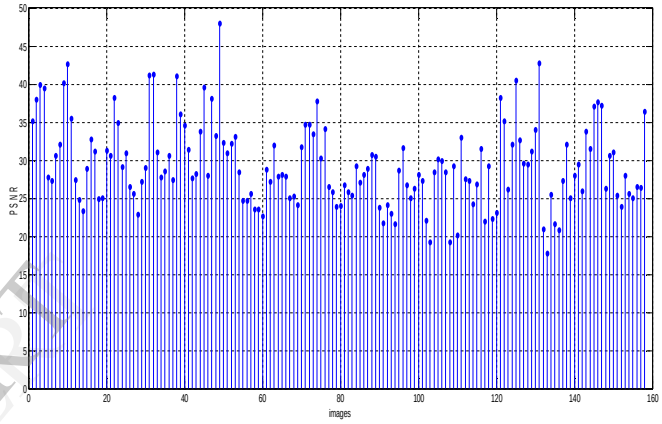

Fig.4. PSNR plot for encrypted images

The performance evaluation factors MSE and PSNR for encryption is obtained from different images are computed and best encrypted images details are summarized with their image number and name is shown in Table. I.

TABLE I. COMPARISON OF MSE AND PSNR FOR DIFFERENT IMAGES

Images	Image Name	MSE	PSNR
49	5536.jpg	1.0	48.0
131	5618.jpg	3.4	42.8
10	5497.jpg	3.5	42.7
32	5519.jpg	4.8	41.3
31	5518.jpg	4.9	41.2

The results show that as the MSE value is increases and PSNR is decreases and the encryption security reduces.

IV. CONCLUSION

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", SPIE Media Forensics and Security XI, Jan. 2009.

[6] A. Gionis, P. Indyk and R. Motwani, "Similarity Search in High Dimensions via Hashing", Proc. of the Int'l Conf. on Very Large Data Bases, 1999.

[7] 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.

[8] 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.

[9] G.-H. Chen, C.-L. Yang, and S.-L. Xie, "Gradient-based structural similarity for image quality assessment", Proceedings of International Conference on Image Processing, Atlanta, GA, pp. 2929–2932, 2006.

[10] F. Wei, X. Gu and Y. Wang, "Image Quality Assessment using Edge and Contrast Similarity", Proceedings of IEEE International Joint Conference on Neural Networks, Hong Kong, China, pp. 852–855, 2008.

[11] G. Zhai, W. Zhang, X. Yang and Y. Xu, "Image Quality Assessment Metrics based on Multi-scale Edge Presentation", Proceedings of IEEE Workshop Signal Processing System Design and Implementation, Athens, Greece, pp. 331−336, 2005.

[12] C.-L. Yang, W.-R. Gao and L.-M. Po, "Discrete Wavelet Transform-based Structural Similarity for Image Quality Assessment", Proceedings of IEEE International Conference on Image Processing, San Diego, CA, pp. 377−380, 2008.

[13] 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, Vol. 15, pp.422–429, 2006.

[14] www-db.stanford.edu/~wangz/image.vary.jpg.tar.

[15] Z. Wang, E. P. Simoncelli and A. C. Bovik, "Multiscale Structural Similarity for Image Quality Assessment", Proceedings of IEEE Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, pp. 1398–1402, 2003.

[16] Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (IJRTE), Vol.1, No.6, Jan 2013.

[17] Somdip Dey, "SD-EI: A Cryptographic Technique To Encrypt Images", Proceedings of "The International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec 2012)", held at Kuala Lumpur, Malaysia, pp. 28-32, 2012.

[18] Parameshachari B D and Dr. K M S Soyjaudah, "Analysis and Comparison of Fully Layered Image Encryption Techniques and Partial Image Encryption Techniques", Proceedings of ICIP 2012, CCIS 292, pp. 599–604, Springer-Verlag Berlin Heidelberg, 2012.

[19] Parameshachari B D and Dr. K M S Soyjaudah "A New Approach to Partial Image Encryption", Proceedings of ICAdC, AISC 174, pp. 1005–1010, Springer India, 2013.