Multimedia Content Security using Image Encryption

Reshu Choudhary
Bhagwant University,Ajmer

Arun JB
TTC, Govt. Polytechnic College,Jodhpur

ABSTRACT
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. Valuable multimedia content such as digital images, however, is vulnerable to unauthorized access while in storage and during transmission over a network. Visual cryptography is a method for protecting image based secrets that has a computation-free decoding process.

In this proposed technique a color images are used, and by applying proposed algorithm image decryption is successfully achieved with satisfactory results. Encrypted Image quality measurement is done with PSNR calculation. MATLAB is used for applying algorithm, simulated results shows that secure image transmission can achieved without revealing information about image content.

Keywords
Secure image retrieval, visual cryptography, image quality measure, feature protection.

1. INTRODUCTION
Now days, more and more digital images are being sent over computer networks and security of these images is major issue. Encryption of images gives one of the solutions to solve it. These techniques try to convert original image to another image so it is difficult to understand and to keeps the image confidential between users and it is important that without decryption key no one can access the content [1]. Image encryption has applications in internet communication, multimedia systems, telemedicine, military communication etc. Information retrieval from encrypted databases is an important technological capability for privacy protection in multiparty information management [2].

Encryption method can be the immediate solution to protect information against hacker or eavesdroppers. Such type of techniques required encryption of an image through some sort of mathematical algorithm where only the real party that shares the image could possible decrypt to use the image [3]. Encryption uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form [4]. These are widely use of images in different-different processes. Therefore, the security of image data from hackers and unauthorized users is important. Image encryption plays an important role in the field of information hiding. Image hiding or encrypting method and algorithm can be very from simple methods to more complicated and reliable frequency method. Mainly available encryption algorithms used for text data and cannot be suitable for multimedia data so there is need to develop image encryption based algorithms. These algorithms use image quality measurement parameters which are important for many image processing applications. Image quality measurement is closely related to image similarity measurement in which quality is based on the differences between a degraded image and the original image. There are two ways to measure image quality by subjective or objective measurement. Subjective evaluations are expensive and time consuming and in real time system it is impossible to implement. Objective evaluations are automatic and mathematical defined algorithm. To validate the usefulness of objective measurements subjective measurement can be used. Therefore objective methods have attracted more attentions in recent years [5]. Well-known image quality 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
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.

In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes have been proposed. The various ideas used in the existing image encryption techniques can be classified into three major categories: position permutation, value transformation and the combination form. The position permutation algorithms scramble the data position within the image itself and usually have low security. On the other hand, the value transformation algorithms transform the data value of the original signal and have the potential of low computational complexity and low hardware cost. Finally, the combination forms perform both position permutation and value transformation and usually have the potential of high security. In recent years, a number of different image encryption schemes have been proposed in order to overcome image encryption problems. A few image encryption techniques suggested recently are discussed in the following paragraph in brief.

In 2010, Yoon and Kim developed a chaotic image cipher in which initially a small matrix was generated using chaotic logistic map [6]. Authors constructed a large permutation matrix from generated small matrixes. The constructed permutation matrix was used to permute plain image pixels. Further, a new chaotic image cipher was suggested by Ismail in which they used two chaotic logistic maps as well as an external secret key of 104-bits size [7]. Control parameters for both chaotic logistic maps were generated from the used external secret key. They also employed a feedback mechanism in their image cipher to make system more secured. In 2011 [8], Jolfaei and Mirghadri suggested a chaotic image cipher based on pixel shuffling, using baker map, and modified version of simplified AES (S-AES), developed by Musa in 2003 [9] . Further, Nayak proposed a chaotic image cipher using logistic map [10]. In the

algorithm, permutation of image pixels was made on the basis of index position of generated chaotic sequence. Sathishkumar and Bagan suggested a chaotic image cipher based in which block permutation, pixel permutation and value transformation were used [11]. Next, chaotic image cipher using two chaotic logistic maps and a secret key of 80-bits was suggested by Chen and Chang [12]. Indrakanti and Avadhani developed a non-chaotic image cipher in which encryption was achieved in three processes. In the last process, a key was generated which keep all information about encryption process [13]. Next, Xin proposed a chaos based cryptosystem based on diffusion and confusion [14].

To improve the security of the confusion module, authors introduced diffusion mechanism in confusion stage through a lightweight bit level permutation algorithm. Peng proposed an image block encryption algorithm based on three dimensional Chen chaotic dynamical systems. The algorithm used a secret key of 192-bit size with an image block of 32-bit long. In the algorithm, Chen's system generated a chaotic sequence that was inputted to a designed function G which was iterated several times [15]. Further, Sathish Kumar suggested an image encryption scheme using multiple chaotic based circular mapping. Based on the initial conditions, each map produces random numbers from orbits of the maps. Among those random numbers, a particular number from a particular orbit was selected as a key for the encryption algorithm. Further, input image was reshuffled and divided into various sub-blocks. Then the position permutation and value permutation was applied to each binary matrix based on multiple chaos maps. Jamei proposed an image encryption using chaotic signals and complete binary tree. In the method, perfect binary tree was utilized to increase complexity in the encryption algorithm. Next, Sathyanarayana designed an encryption algorithm focusing on the application of properties of finite fields and elliptic curves. Additive and Affine encryption schemes using six schemes of key sequences obtained from random elliptic curve points were designed. Pareek proposed a lossless digital image encryption scheme based on the permutation and substitution architecture. In the algorithm, plain image was divided into squared sub-images and then reshuffled them. Further, in the permutation process a simple arithmetic, mainly sorting and differencing, was performed to achieve the substitution.

Hybrid model of cellular automata and chaotic signal was proposed for image encryption by Fateri and Enayatifar .In this method, 8-bits mask was used for changing the pixel gray level of main image. For changing each pixel gray level, value of each bit of the mask was selected by one of the 256 cellular automat standard rules. One of the 256 cellular automat standard rules was determined by chaotic signal.

2.1 Image Evaluation Techniques

Some image encryption and decryption quality are measured by researches most commonly used parameters are:

2.1.1 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 [15-21]. 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:-

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

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×N image. MSE is zero when $x(i, j) = y(i, j)$.

2.1.2 Peak Signal to Noise Ratio (PSNR)

The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error.

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

If PSNR value is high it shows good quality image [15-21].

3. PROPOSED TECHNIQUE

The new algorithm of this paper handles hiding different images inside other images of various types. When an image is chosen to be used for hiding other image, it is called a cover image. The encrypted image produced by encryption of cover image and secret image leave some sign of encryption like visual presentation 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. In this method cover image plays a role of key. The encrypted image is not identified by hackers and not by any mathematical tool if cover image is not present [22]. In this proposed technique we introduced two methods and evaluate overall improvement in image quality.

3.1 Method (A)

In this method two images are selected as a cover image and secret image and adding them for generating encrypted image.

$$\text{Method A(Encrypted image)=Image 1+Image2} \quad (3)$$

where Image1 is cover image and Image2 is secret image. Get decrypted image by again subtracting cover image by encrypted image.

3.2 Method (B)

In this method again two images are selected and apply following method over it:

$$\text{Method B(Encrypted image)=Image1+((Image2)*0.5)} \quad (4)$$

where Image1 is cover image and Image2 is secret image.$PSNR_1$ 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.

TABLE I
COMPARISON TABLE FOR METHOD A AND METHOD B

Image	Method A[25,26]				Method B				% Improvement			
	$PSNR_1$		$PSNR_2$		$PSNR_1$		$PSNR_2$		$PSNR_1$		$PSNR_2$	
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
	17.10	48.06	15.12	23.17	18.12	51.39	21.04	26.68	05.9	06.9	39.2	15.2
	11.28	46.27	09.54	18.86	12.56	51.27	15.50	22.23	11.4	10.8	62.5	17.9
	09.94	35.63	08.06	17.71	10.63	51.24	13.98	19.99	06.9	43.8	73.5	12.9
	24.43	∞	21.02	24.86	25.38	51.44	26.89	29.81	03.9	-	27.9	19.9
	17.32	56.34	14.94	22.22	18.50	51.78	20.89	25.18	06.8	-8.1	39.8	13.3
	27.74	∞	26.82	37.78	28.26	51.67	32.61	41.24	01.9	-	21.6	09.2
	08.61	37.79	07.08	17.89	09.63	51.37	13.05	20.42	11.9	35.9	84.3	14.2
								Average Improvement	**07.0**	**17.9**	**49.8**	**14.7**

This proposed technique adding encryption to a color picture, through adding color cover image with secret color image. It 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. It uses only images having size of 128×96 (w×h) pixels, total number of pixels are 12288 [23]. It is compared with other method which is given by Abdelfatah A. Tamimi and Ayman M. Abdalla in which they use smaller secret image size than the cover image size [24]. This difference is nearly 200 times which bring more burdens on transmission network due to their large size. In our method cover image and secret image size is same and it efficiently encrypted.

By these two methods we find quality Improvement in hiding the information. In method B there are minimum distortion comparatively method A therefore detection becomes difficult. Overall improvement in Min for $PSNR_1$and $PSNR_2$ is 49.8 % as shown Table I. One Quality is improved by $PSNR_1$ is Max and $PSNR_2$ is Min. By this algorithm there is significant improvement in minimum $PSNR_2$ having average of 50% varies from 21.6 to 84.3.

4. CONCLUSIONS

Requirement of digital images in multimedia transmission over network is important in image processing. For this purpose evaluation of transmitted image is important. This proposed method use same size of color images to encrypt and decrypt images directly for real time applications. This proposed technique provides good selection of key image by which successful cryptography is achieved. An extensive study of security and performance analysis of the proposed image encryption technique using various statistical analysis, key sensitivity analysis, differential analysis, key space analysis, speed performance, etc. have been carried out. Based on results of analysis, it is concluded that the proposed image encryption technique is perfectly suitable for the secure image storing and transmission.

5. 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] Ji Won Yoon and Hyoungshick Kim, "An Image Encryption Scheme with a Pseudorandom Permutation Based on Chaotic Maps", Communication in Nonlinear

Science and Numerical Simulation, Vol. 15, No. 12, pp. 3998-4006, 2010.

[7] Ismail Amr Ismail, Mohammed Amin and Hossam Diab, "A Digital Image Encryption Algorithm based a Composition of two Chaotic Logistic Map", International Journal of Network Security, Vol. 11, No. 1, pp. 1-10, 2010.

[8] Alireza Jolfaei and Abdolrasoul Mirghadri, "Image Encryption using Chaos and Block Cipher", Computer and Information Science, Vol. 4, No. 1, pp. 172-185, 2011.

[9] M. Musa, E. Schaefer and S. Wedig,"A Simplified AES Algorithm and its Linear and Differential Cryptanalysis", Cryptologia, Vol. 27, pp. 148-177, 2003.

[10] Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das, "Image Encryption using an Enhanced Block based Transformation Algorithm", International Journal of Research and Review in Computer Science, Vol. 2, No. 2, pp. 275-279, 2011.

[11] G.A. Sathishkumar and K. Bhoopathy Bagan, "A Novel Image Encryption Algorithm using Pixel Shuffling Base 64 Encoding based Chaotic Block Cipher", WSEAS Transactions on computers, Vol. 10, No. 6, pp. 169-178, 2011.

[12] Dongming Chen and Yunpeng Chang, "A Novel Image Encryption Algorithm based on Logistic Maps", Advances in Information Science and Service Sciences, Vol. 3, No. 7, pp. 364-372, 2011.

[13] Sesha Pallavi Indrakanti and P.S. Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications, Vol. 28, No. 8, pp. 45-47, 2011.

[14] 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.

[15] 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.

[16] 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.

[17] 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, pp. 377−380, 2008.

[18] 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 .

[19] 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, pp. 1398–1402, 2003.

[20] 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), Vol. 1, No. 6, Jan 2013.

[21] 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.

[22] Arun JB and Reshu Choudhary, "Image Encryption for Secure Data transfer and Image Based Cryptography",International Conference on emerging trends of Research in Applied Science and Computational Technique, Feb 21-22, 2014.

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

[24] Abdelfatah A.Tamini and Ayman M.Abdalla, "Hiding an Image inside another Image using Variable-Rate Steganography", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013.

[25] Reshu Choudhary and Arun JB, "Secure Image Transmission and evaluation of Image Encryption", Subbmitted in: IEEE International conference on Recent Advances and Innovations in Engineering, 2014.

[26] Reshu Choudhary and Arun JB, "A Secure Image Transmission with Improved Encryption Technique", Accepted in : National Conference in Wireless Communication and Artificial Intelligence, 2014.