Analysis of Palm print Based Image Encryption Technique Using DES Approach

Swati Verma , Abhishek Misal
Department of Electronics & Communication Engineering,
Chhatrapati Shivaji Institute Of Technology, Durg (C.G), India
swatiiverma09@gmail.com
abhishekmisal@csitdurg.in

Abstract- **Encryption is used to disguise data making it unintelligible to unauthorized observers. Providing such security is especially important when data is being transmitted across open networks such as the internet. Since, image data have special features such as bulk capacity, high redundancy and high correlation among pixels that imposes special requirements on any encryption technique. This paper presents image encryption/ decryption scheme using biometric template (Palm Print) by generating cryptography key. Encryption and Decryption process takes place by using cryptography algorithm i.e. DES (Data Encryption Standard. The proposed scheme is especially useful for encryption of large amounts of data, such as digital images. This scheme satisfies the characters of convenient realization, less computation complexity and good security. Experimental results show better encryption technique in terms of security against statistical attack i.e correlation, PSNR and entropy values for different file format images and also show the histogram of original image and encrypted image.**

Keywords: **Image processing, Biometric, image encryption and decryption, Palm Print.**

I INTRODUCTION

With the proliferation of the internet and maturation of digital communications, applications of digital imaging are prevalent and are still continuously and rapidly escalating today. A key hindrance in widespread deployment of digital image services is to enforce security and ensure authorized access to sensitive data in transit. Modem digital communication enables the transmission of bulky data to far off places over public network. This data is not only text but also includes video, image, voice and music. Image and video contents are equally preferred because of their information implicative property. Security of these images become even more critical when they are medical images/x-rays, military emplacements or confidential data belonging to sensitive agency [12][13]. Such critical information should be protected during transmission from eavesdroppers. Most of the existing encryption algorithms are best suited for textual data and cannot directly be applied on images because of intrinsic characteristics of images such as strong correlation among pixels, bulk data capacity and high redundancy. Therefore, image security has its own special requirements [13][14][15] that leads to three different schools of thoughts to protect digital data. The main idea behind the present work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. A study of image compression is becoming more important since an uncompressed image requires a large amount of storage space and high transmission bandwidth noise. Because of the proposed scheme based on Digital Encryption Standard, it is easily implemented and highly efficient to quickly encrypt and decrypt image messages. The symmetric encryption mechanism makes the encrypted data more secure.

The rest of the paper is as follows. Section 2 surveys on some related image cryptosystems. Section 3 describes steps for generating cryptography key process of encrypting original image by using DES encryption algorithm and then decrypting them. Experimental results and Statistical Analysis are given in section 4 and section 5, respectively. Section 6 deals with conclusion. Biometric-based authentication system should be designed to withstand attacks when deployed in security critical applications such as e-commerce and accesses to restricted data/buildings. The biometric-based encryption requires physical presence of persons to be authenticated and is therefore reliable, convenient and efficient. The encryption keys in are generated using low-level combination of biometric features and cryptology. Reliability in computer aided personal authentication is becoming increasingly important in the information-based world, for effective security system. Biometrics is physiological characteristics of human beings, unique for every individual that are usually time invariant and easy to acquire. Palm print is one of the relatively new physiological biometrics due to its stable and unique characteristics. The rich information of palm print offers one of the powerful means in personal recognition.

II SURVEY ON RELATED IMAGE CRYPTOSYSTEMS

According to the differences between image and text, recently there have been several innovative encryption techniques:

2.1 A Technique for Encryption

An iterative speech encryption scheme basis of subspace method was proposed by Atef Mermoul. Blind source separation (BSS)-based encryption schemes have been built up using the intractability of the under determined BSS problem. In this paper, the author designed a novel encryption

scheme that is iterative and based on the idea of subspace technique, by the nonlinear functions and the key signals. It is proved here that only a part of the secret key parameters were used in encryption process is needed for the decryption process. Also this technique gives no contents if no plain-text is fed in the input [1].

Mort Naraghi-Pour and his colleagues have developed a simple encryption standard for secure detection in the wireless sensor networks. Only the authorized user or the ally fusion center (AFC) is aware of the encryption method its features, and no unauthorized or any third party fusion centers (TPFC) are not aware of such encryption features. As the result shown, the exact threshold value was found and the numerical results were evaluated for the error probabilities of the two fusion centers (AFC and TPFC) [2].

A Study on OMAP (Open Multimedia Applications Platform) Digital Fingerprint Encryption technique has done by Zhu Yuxi. In this study the author deals with the identification of the fingerprint and the security in transmission for the embedded systems. Here a digital fingerprint technique was used with the structure of the OMAP (Open Multimedia Applications Platform). The author designed an integrated software structure with an application platform [3].

Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor has jointly framed a manuscript for Classifying the Encryption Algorithms in accordance with the Pattern Recognition method. In this discussion the authors focuses on the limitations of the algorithms which are used for encryption scheme and for generating the keys for encryption process. Here the pattern recognition method to identify the block ciphers in encryption process. The block cipher algorithms like AES, DES, IDEA, and RC were used to identify the good classification technique. As the result shown, that the performance of RoFo (Rotaion Forest) classifier has the very good classification accuracy [4].

2.2 Stream Encryption

Ai-hongZhu and Lia Li presented a new algorithm that produced nine chaotic sequences only by one secret-key, six sequences were used to scramble the position of image pixels, and the others were used to confuse and diffuse image pixels value [5].

2.3 Image encryption

Analysis on encryption techniques with JPEG Images was done by W. Puech, and J.M. Rodrigues. This paper mainly focuses on the draw backs of both the selective encryption (SE) and the image compression. The SE (selective encryption) can be made by Advanced Encryption Standard (AES) algorithm incorporate with the Cipher Feedback (CFB) mode. And for the compression, the JPEG algorithm has been used. Here the SE was done in the stage of Huffman coding in JPEG algorithm which does not affects the size of the compressed image. The results shows the application of SE in JPEG compressed images [6].

Mahmood Al-khassaweneh and Selin Aviyente has put forth a novel image encryption technique based on the concept of Least Square Approximation (LSA) .In this paper, the conversion of the original image into the form of encrypted one by the randomly generating vectors. And on the other hand the original image has been decrypted by using the least square approximation concept on the encrypted image and also on the randomly generating vectors. As the result of this, there is a good range of efficiency in this algorithm and also promotes good enhancement in the security aspects [7].

Seyed Hossein Kamali et al have framed an image encryption algorithm of enhanced model of Advanced Encryption Standard. The authors proposed an enhanced model of Advanced Encryption Standard to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original AES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks [8].

2.4 Double Encryption

A new double random phase encryption method has been proposed by Ayman Alfaloul, and Ali Mansour to multiplex and simultaneously encodes multiple images. This method can enhance the level of encryption of a classical “DRP” Double Random Phase encryption system this promotes a very simple implementation, robustness, and can easily apply on various image formats. This technique deals with two tiers. The first tier is multiplexing which performs iterative Fourier transformations together with several encryption key-images. And the second tier is classical DRP system. Both the tiers produce encoding of several target images and reduces the time and storage complexity [9].

2.5 A New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo [10] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image’s pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point x(0), row size M and column size N of the image f, iteration number no, and constants Á, ?, and µ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels [11].

2.6 Visual Cryptography for Colour Images

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Young-Chang

Hou [12] has proposed three methods for visual cryptography. All these proposed methods belong to symmetric key cryptosystem, they are vulnerable in case they employ the unique key in their proposed system (Jinn- Ke Jan, 1996). Here, we propose a novel symmetric image encryption scheme. Our method can achieve the following two goals. One is that it is easily implemented and highly efficient to quickly encrypt and decrypt image messages based on DES and generating encryption and decryption key using Canny Edge Detection method. The other is that symmetric encryption mechanism makes the encrypted data more secure.

III ENCRYPTION & DECRYPTION

We consider encrypting the color image in different file format (.jpg, .png, .tiff, .bmp etc.). The complete encryption process is described as follows:

Step 1: Loading the colored digital image.

Step 2: Taking biometric template (palm print) from database for key generation.

Step3: Generating encryption key (k_e) by using canny edge detection method. In this technique Num and Eul values are obtained. Num defines the number of connected edges and Eul defines the total area of palm print. An array is then created for both Num and Eul having prime numbers starting from 1 to the respective values. The arrays are denoted as Prime Num ( ) and Prime Eul ( ). Then the size of both arrays is calculated and stored in dim (1) and dim (2) for Num and Eul respectively. Then Mod |5| for dim (1) is calculated. The calculated Mod |5| value for dim (1) indicates the element from start of the array in Prime Num ( ) from where, consecutive 4 prime numbers are taken and stored as array "a" where a = num (4 consecutive prime numbers of Prime Num ( ) starting from the element selected by Mod |5| value of dim (1)).
Similarly, Mod |5| for dim (2) is calculated. It is evident that both Prime Num ( ) and Prime Eul ( ) will have some common prime numbers. These common prime numbers have now been discarded in array Prime Eul ( ). The calculated Mod |5| value for dim (2) indicates the element in Prime Eul ( ),after discarding common prime numbers, from where, consecutive 4 prime numbers are taken and stored as array "b",
where b = eul (4 consecutive prime numbers of PrimeEul ( ) starting from the element selected by Mod |5| value of dim (2) after discarding common prime numbers).
The 4 numbers obtained from both array a and b are in decimal form. These values are then converted into 8 digit binary form. Thus we have obtained 32 bit from both array a and b. This will give the Key of 64 bits.

Step 4: Encrypting already loaded colored digital image using DES algorithm with the help of key (k_e) generated in above step.

Step 5: Encrypted image/cipher image is generated.
The complete decryption process is described as follows:

Step 1: Loading the encrypted image generated in encryption process.

Step 2: Taking the same biometric template (palm print) from the database for key generation.

Step 3: Generating decryption key (k_d) by using Canny Edge Detection method as discussed in encryption process.

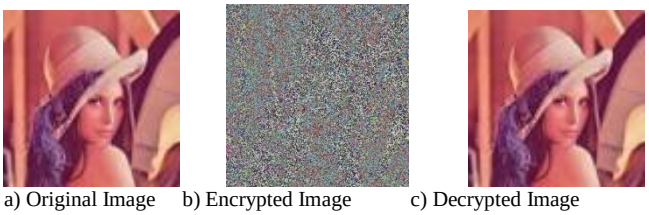
Step 4: Matching of key: If the encryption key matches the decryption key i.e.$k_e = k_d$, then only the process of decryption takes place to get the decrypted image or output image which is also known as the original image or input image, otherwise if ke≠kd then a message showing "password not authenticate" will appear after implementing this process in MATLAB.

Step 5: If encryption key is same as decryption key ($k_e = k_d$), then the process of decryption occurs using DES algorithm.

Step 6: Decrypted/original image is obtained.

IV EXPERIMENTAL RESULT

The DES image encryption algorithm using biometric template (palmprint) is tested and evaluated based on software simulation in MATLAB 12a. Results of some experiments are given to prove its efficiency of application to digital images. We use several images as the original images (plain images). The encrypted images are depicted in Figs. 1b-2b. As shown, the encrypted images (cipher image) regions are totally invisible. The decrypted images are shown in Figs. 1c-2c. The visual inspection of Figs. 1-2 shows the possibility of applying the proposed Image crptosystem successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.



a) Original Image b) Encrypted Image c) Decrypted Image
Figure 1: DES based Image Cryptosystem using palmprint applied to Lena image

a) Original Image b) Encrypted Image c) Decrypted Image
Figure 2: DES based Image Cryptosystem using palmprint applied to another colored image.

V STATISTICAL ANALYSIS

(1) PSNR (Peak signal to Noise Ratio)

The noise immunity reflects the ability of the image cryptosystem to tolerate noise. To test the noise immunity, noise with different signal to noise ratios (SNRs) is added to the encrypted image, and then the decryption algorithm is performed. If the decrypted image is close to the original image, we can say that the cryptosystem at hand is immune to noise. This closeness can be verified visually or numerically with the value of r xyd , which represents the correlation coefficient between the original image and the decrypted image, and the peak signal to noise ratio (PSNR) of the decrypted image, which is defined as follows

$$PSNR = 10\times \log_{10}\left(\frac{M\times N\times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}|(f(m,n)-f_d(m,n)|}\right) \quad (1)$$

where f (m, n) is the original image and , f_d (m n) is the decrypted image.

(2) Correlation

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipherimages. This metric can be calculated as follows:

$$r_{xy} = \frac{conv(X,Y)}{\sqrt{D(X)\sqrt{D(Y)}}} \quad (2)$$

where x and y are the gray-scale values of two pixels at the same indices in the plain and cipherimages. In numerical computations, the following discrete formulas can be used:

$$E(X) = \frac{1}{L}\sum_{i=1}^{L} X_i \quad (3)$$

$$D(X) = \frac{1}{L}\sum_{i=1}^{L}(X_i - E(X))^2 \quad (4)$$

$$Cov(x,y) = \frac{1}{L}\sum_{i=1}^{L}(X_i - E(X)(Y_t - E(Y)) \quad (5)$$

where L is the number of pixels involved in the calculations. The closer the value of r xy to zero is, the better the quality of the encryption algorithm.

(3) Information entropy analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [16]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy H (m) of a source m, we have:

$$H(m) = \sum_{i=0}^{2^N-1} P(m_i)\log_2(1/P(m_i)) \quad (6)$$

Where $P(m_i)$ represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e., m = {m1,m2 ,...,m28 }after evaluating Equation, we obtain its entropy H(m) = 8 , corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Table 1 above shows the calculated values of PSNR, Correlation and Entropy for 10 digital images and respective graphs are shown in figure 3 and 4.

TABLE I
Values of different parameters based on statistical attack

Image No.	Format	PSNR	Correlation	Entropy
1	.jpg	255	0.955	7.745
2	.jpg	255	0.958	7.359
3	.jpg	255	0.966	7.759
4	.jpg	255	0.985	7.671
5	.jpg	255	0.999	7.557
6	.jpg	255	0.937	7.70
7	.png	255	0.955	7.662
8	.jpg	255	0.926	7.864
9	.jpg	255	0.964	7.386
10	.jpg	255	0.893	6.159

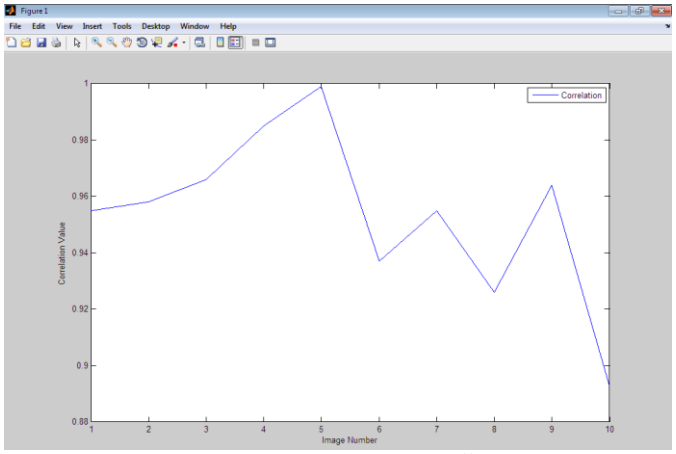


Figure 3: Correlation Graph between 10 different Images

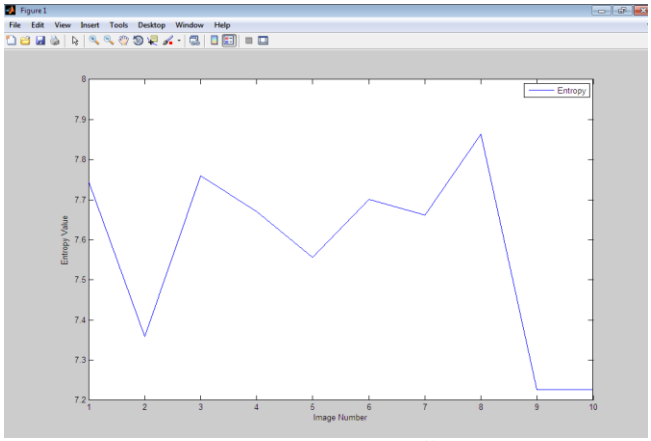
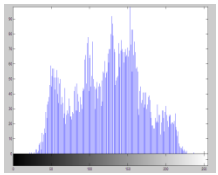


Figure 4: Entropy Graph between 10 different Images

(4) Histogram

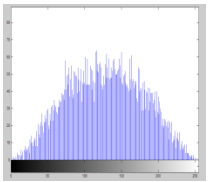
To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig.3b. The histogram of a Lena image contains large spikes. The histogram of the cipher image as shown in Fig.3d, is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure. [16-17].

a) Original Image



b) Histogram of original image

c) Encrypted Image



d) Histogram of encrypted image

Figure 5: Histograms of Lena original image and ciphered image. in .jpg format in which (a) shows original image (b) shows Histogram of original image (c) shows Encrypted image (d) Histogram of Encrypted Image.

VI CONCLUSION

In this paper, we present a new private-key encryption scheme based on palm print. We presented a new encryption/decryption scheme based on palm print. Our scheme allows one party to send a secret image to another party over the open network, even if many eavesdroppers listen. Therefore, our scheme can be useful in many applications. Biometric based cryptographic key generation is proposed and generated cryptographic key is given to the encryption/decryption block where the process of encryption/decryption takes place with the help of DES Algorithm. Experiment results indicate that the proposed algorithm performs well and successfully encrypts and decrypts the image. The values calculated are tabulated in Table 1 shows the PSNR, Entropy, Correlation Coefficient of 10 images. Few readings were found to have deviations from the desired results. Also, experimental results show the Histograms of two different images and its encrypted images that indicate that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure. The experimental results have showed that the generated 64-bit cryptographic key is capable of providing better user authentication and better security against statistical attacks.

REFERENCES

[1] Atef Mermoul, "An Iterative Speech Encryption Scheme Based On Subspace Technique" IEEE Transactions on Systems, Signal Processing and their Applications, pp. 361-364, 2011.

[2] Mort Naraghi-Pour, Venkata Sriram Siddhardh Nadendla," Secure Detection in Wireless Sensor Networks Using a Simple Encryption Method" IEEE Transactions, 2011.

[3] Zhu Yuxi, Ruchun Cui, "Applied Study Based on OMAP Digital Fingerprint Encryption Method" IEEE Transactions pp. 1168-1172, 2010

[4] Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor ,"Classifying Encryption Algorithms Using Pattern Recognition Techniques" IEEE Transactions pp. 1168-1172, 2010

[5] Ai-hongZhu, Lia Li, ―Improving for Chaotic Image Encryption Algorithm Based on Logistic Map‖, 2nd Conference on Environmental Science and Information Application Technology, 2010.

[6] W. Puech, J.M. Rodrigues," Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images" IEEE Transactions on Image Analysis for Multimedia Interactive Services, , 2007.

[7] Mahmood Al-khassaweneh, Selin Aviyente,"Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.

[8] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard(AES) Based Algorithm for Image Encryption", IEEE Transactions on Electronics and Information Engineering, Vol 1,pp.141-145,2010

[9] Ayman Alfalou and Ali Mansour, "A new double random phase encryption scheme to multiplex and simultaneous encode multiple images" Applied Optics, pp. 5933-5947, 2009.

[10]. S. Ribaric and I. Fratric, "A biometric identification system based on Eigenpalm and Eigenfinger features", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 1698-1709, 2005.

[11]. A. Okatan, C. Akpolat and G. Albayrak, "Palmprint verification by using cosine vector", IJSIT Lecture Note of International Conference on Intelligent Knowledge Systems, vol. 1, no. 1, pp. 111-113, 2004.

[12]. W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," Pakistan Journal of information and Technology. Vol. 2, no. 2, 2003, pp. 191-200.

[13]. M. Salleh, S. Brahi and I. Fauzia Isnin, "Image Encryption Algorithm Based on Chaotic Mapping," Journal Technology 39(D) Dis. 2003: 1-12 [14]. M. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," in ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision
Systems, 2002
[15]. S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," proceeding of lASTED international conference, single processing, pattern recognition and application, 2002, pp. 25-28.
[16] J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.
[17] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48 (8), 2439–2451, 2000. affiliation

