MANTECH Publications

Journal of Digital Image Processing and Computer Vision
Volume 3 Issue 1

Security and Privacy Protection on Image-A Survey

Jeena Johnson[1], Josna Jose[2]
Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
College of Engineering kidangoor, kottayam, Kerala
Corresponding Authors' email id: *jeenajohnson93@gmail.com*

Abstract

This paper focuses on different kinds of image encryption and decryption technique. In addition focuses on the image encryption technique. There are various techniques which are discovered from time to time to encrypt and decrypt the image to make more secure. Video surveillance system are becoming omnipresent. Visual surveillance has emerged as an effective technology for public security, privacy has become an issue of great concern in the transmission and distribution of surveillance video. Various encryption methods and scrambling methods are used to protect the facial biometric components and also various method are to be used facial biometric verification. The main intension of this paper is functionality of image encryption and decryption techniques mainly present the FFL scheme for verify the facial biometric components.

Keywords: *Face scrambling; Encryption; Decryption; Privacy; fuzzy random forest; fuzzy decision tree*

I. INTRODUCTION

Face recognition is increasingly deployed as a means to unobtrusively verify the identity of the people .Image data are frequently shared and stored in worldwide at various end to end. The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image especially in video surveillance. Encryption is the process of transforming information so it is unintelligible to

anyone but intended recipient. Decryption is the process of transforming encrypted image so that it is more intelligible again. Image encryption algorithm can be classified into three categories 1) position permutation based algorithm [15] 2) value transformation based algorithm 3) visual transformation based algorithm [15]. Face recognition has been focus of the research community due to its unobtrusiveness and ease of use. Image scrambling is widely applied in digital image watermark technology. Therefore Arnold transform is often used, but its security is not enough because the form is only and public. In presence the improved Arnold transform is present. It is realized in computer through proving.

Currently there are many methods for calculating the periodicity of Arnold transformation and getting the inverse Arnold transform. The use of traditional Arnold transformation for image scrambling has become unsafe, for this issue it proposes an algorithm for digital image block location scrambling. There are different ways to perform scrambling. 1) scrambling can done simply by masking or cartooning[1].

In this kind of scrambling will lose the facial information and in this case face recognition become unsatisfied or unsuccessful. 2) Arnold transform is the another method for scrambling the image above mentioned. 3) New digital image scrambling method based on Fibonacci number 4) Transform-domain scrambling is applied in MPEG-4 Motion JPEG 2000

II. LITERATURE SURVEY

1. New Mirror-Like Image Encryption Algorithm and VLSI architecture

Jiun-In Guo et al [15] have proposed an algorithm it was mirror like. There are 7 steps included in it. In initial step 1-D chaotic system is determined and its initial point x (0) and set k=0. Next the chaotic sequence is produced from chaotic system. Then binary sequence is also generated from chaotic system. Last four stages picture elements are rearranged using swap function according to the binary sequence.

2. Techniques for Image Encryption using Digital Signature

Aloka Sinha et al [14] proposed a new method in which the digital signature of the original image is added to the encoded version of the original image. A very suitable error code is followed to do encoding of the image. Ex: BCH code. At the receiver side, after decryption of that

image and the digital signature verify the authenticity of the image.

3. Multilevel and image dividing technique

Chang-Mok shin et al [12] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same gray-level multi-level image is divided into binary images. Then binary pictures is reproduced to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation.

4. Image encryption using ID chaotic map

Fethi Belkhouche et al [11] used the method that can be used binary image encryption with the possibility of using several keys.

5. Image scrambling method based on Fibanocci number

This method [10] includes that standardization and periodicity of scrambling transformation. The advantages of the scrambling transformation are, 1) Encoding and decoding is very simple 2) it is applied in real situation 3) it is very sensible. The data of image are redistributed randomly across the whole image. The method persists common image attacks,such as compression, noise(unwanted signals) ,loss of data packets. This can also develop the video scrambling and probe corresponding embedding algorithm for digital watermark.

6. New modified version of Advanced encryption standard based algorithm for image encryption

Kamali S,H et al presented a modification to the advanced encryption standard (MAES) to provide a high level security and better image encryption. The result shown by them was a higher than that of original AES encryption algorithm

7. Image security via genetic algorithm

Rasul Enayatifar et al [8] proposed that a new method based on a hybrid model composed of a genetic algorithm and chaotic function for image encryption. In their technique, first a number of encrypted images are construction using the original image with the help of chaotic function. In the next stage these encrypted images are employed as the initial population for starting the operation of genetic algorithm. Then the genetic algorithm is used to optimize the encrypted images as much as possible. In

the end the best cipher-image is chosen as the final encryption image.

8. Statistical analysis of S-box in image encryption application based on majority logic criterion

Tariq Shah et al [6] propose a criterion to analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption application. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine(APA), gray, and Xyi Sboxes.

9. Image encryption using differential evolution approach in frequency domain

Ibrahim S I Abuhaiba et al [5] present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. In order to demonstrate the security of new image encryption algorithm, key space analysis, statistical analysis, and key sensitivity analysis was carried out them.

10. Image encryption based on Bit-plane Decomposition and Random sampling

Qiudong Sun et al [4] general random scrambling method was designed which has more suitable method was designed which has more stable scrambling degree than the classical method classical method Arnold transform. At first they decomposed a gray image into several bit-plane images. Then we shuffled them by a random scrambling algorithm separately. Lastly we merged the scrambled bit-plane images according to their original levels on bit-plane and gained an encrypted image. Due to each bit-plane image is scrambled by using different scrambling random sequences, the bit located at the same coordinate in different bit-planes are almost not stay on the original positions when each bit-plane being scrambled separately, for each pixel its all bits of gray level , therefore, may be come from those pixels located different positions. Consequently, the reconstructed gray levels of image are changed ineluctable. It is obvious can do position exchange scrambling and gray level change scrambling at the same time.

11. Transform domain scrambling and chaotic system

Traditional permutation encryption algorithm is not robustness for noise

disturbing. An image encryption algorithm is based on location transformation. The algorithm encrypts the image based on chaotic system and stores the pixel values in multiple locations. The unique property of chaotic function gives its way to image encryption. A new combined technique is given in [3] which has better chaotic behaviour than traditional ones.

Video coding schemes are also based transform coding. Frames are transformed using an energy compaction transform such as DCT or DWT. The resulting coefficients are then entropy coded using technique such as arithmetic coding. We consider more explicitly two video coding schemes namely MPEG-4 And Motion JPEG 2000.

12. Key based Image scrambling In Transform domain

This method proposed that the image scrambling involving both the spatial as well as transform domain. As we know whenever the transform is applied to an image, image is converted from spatial domain to transform domain and transform coefficients are obtained. To obtain the original image the inverse transform is applied to the transform coefficients. But if the transform coefficients are affected due to any transform we not obtain the original image. Key based scrambling which is based on the random numbers generation based on the size of the image is used for scrambling purpose.

12.1 Steps used for scrambling

1) Read the image, convert into grayscale

2) Apply a transform on the image

3) Transform coefficients which are obtained in step 2 are now scrambled using key based scrambled method.

4) Apply inverse transform on the scrambled transform coefficient obtained in step 3

5) The image obtained in spatial domain will now be scrambled.

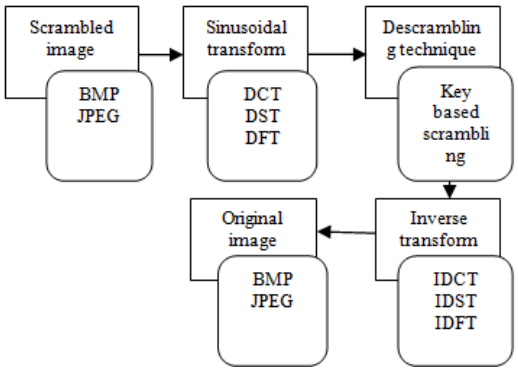

Fig1. De-scrambling process (Image taken from [2])

12.2. Descrambling Steps

1) Read the scrambled image

2) apply the transformation on the image

3) Transform coefficients which are obtained in step 2 are now descrambled using key based descrambled method.

4) Apply inverse transform on the descrambled transform coefficient obtained in step 3

5) The image obtained in spatial domain will now be original image.

13. Scrambling

In comparison with encryption, image scrambling has two advantages.1) scrambling usually has much lower computation cost than encryption making it suitable for computing efficient network target application. 2) Encryption may undermine the purpose of public security control because its decryption depends upon the acquiring encryption key. For example a security guard who needs to check a key face in surveillance video may not be able to do he/she has the decryption key. In comparison, scrambled face using the Arnold transform can be easily recovered by manual attempts using the inverse Arnold transform with different parameter.3) This algorithm can achieve good encryption effect. 4) it has large key space. 5)Key sensitivity.6) it is basically meets effectiveness. 7) Provide security requirements of image encryption. 8) Simplicity and ease of use.

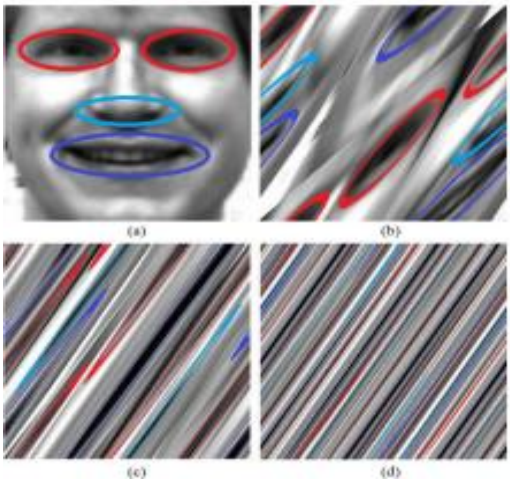

Fig2.Face scrambling using Arnold transform (a)semantic facial components.(b) after one Arnold transform.(c) after two Arnold transform.(d)after three Arnold transform(Image taken from [1])

13.1 Inverse Arnold transform

The image can shift by rows and columns by whatever the number specify. Get the image in four image section by running the program, it is possible that some function have changed over the year. However it would be easy to fix it if we can figure how many rows and columns it shift by.

Start with a very small say 8*8 image and see how it changes we get the inverse(it is a 8*8 matrix here) and the amount of shifting . we can undo this two lines of code we have the original image. The advantage of this method is, it basically meets the effectiveness.

Disadvantages are, 1) it is not work with properly especially with inverse operation. 2) when the gray scale image is inverse. It looks like the image is divided into two halves and the first half comes at the bottom and second half appears on the top. 3) iteration count is 10. 4) face recognition has to be a pure data-driven classification issue without using semantic facial components or applying 2D/3D face models to the scrambled image.

To find an effective method for this randomly scattered distortion, Richard jiang et al [1] introduces a fuzzy random forest learning scheme. In this method a random subspace sampling method is applied to extract a subset of features for each fuzzy decision tree.

Such random sampling is expected to overcome the scattered distortion and effectively carry out face recognition on a sparse set of features.

13.2 Fuzzy forest learning

To extract the features from the scrambled face image is robust, a biased random sampling scheme is applied to construct the fuzzy decision trees from randomly selected features. Then a fuzzy forest decision is obtained from all fuzzy trees by the weighted combination of their fuzzy decision vectors of membership.

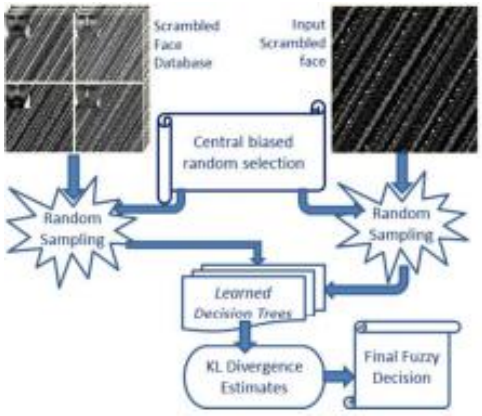

Fig 3.Fuzzy forest learning process (Image taken from [1])

Fig 3 shows an overview of FFL scheme for the scrambled face verification. Given a training dataset, faces are scrambled and forwarded to the FFL scheme. The procedure then randomly selects the features from the scrambled domain with biased weights towards central features, and a number of fuzzy trees are constructed based on the selected features, where LSDA method is applied to extract discriminant features from randomly selected features. After a scrambled face is

input a as test, each tree computes a fuzzy vector of membership and forwarded it to the forest decision process. Final decision is based on a fuzzy combination of all trees.

The advantages of this method, 1) the experiments using three public datasets have successfully validated that the FFL scheme can robustly cope with challenging tests in the scrambled domain. 2) it is worth highlighting that this approach is not dependent on any semantic face models or 3D templates. 3) face specific features targeted toward semantic or 3D face modeling can enhance accuracy.4) face modeling from images and facial component detection needs extra computation time and easily introduce errors. 5) this approach is based purely on data driven and can easily be applied to other similar chaotic pattern classification cases such as texture classification in image analysis or factor analysis of stock prices. 6) the advantages of this approach were that it provide higher classification performance with lower computational cost than decryption. 7) in the case of time, given N classes and K trees, the decision from a tree can be repeated K/N times by random choice.

III. CONCLUSION

The security of image is very important in this internet world. In this paper I have surveyed different image encryption techniques and decryption techniques. Each technique is unique in its own way. Newly proposed image encryption and also enhance the security level by introducing more than one chaotic scheme for image encryption algorithm, In decryption side, A new algorithm of FFL scheme is used to verify the biometric facial components.

REFERENCES

I. Richard Jiang, Ahmed Bouridane, Senior Member, IEEE, Danny Crookes, Senior Member, IEEE," Privacy-Protected Facial Biometric Verification Using Fuzzy Forest Learning",2016

II. H. B. Kekre, Tanuja Sarod, Pallavi N Halarnkar, Debknya Mazumder, "Comparitive performance of image scrambling in transform domain using sinusoidal transforms" ,2014.

III. H.zhu,C.zhao and X.zhang,"A novel image encryption compression scheme using hyper chaos and Chinese remainder

theorem",Image communication, vol 28,2013,pp.670-680

IV. Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University , vol. 09 IEEE, 2012.

V. Ibrahim S I Abuhaiba , Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach In Frequency Domain" , Signal & Image Processing An International Journal (SIPIJ) Vol.2, No.1, March 2011.

VI. Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion", International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011.

VII. Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011

VIII. Rasul Enayatifar , Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.

IX. Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006

X. Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number,"Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.

XI. Fethi Belkhouche and Uvais Qidwai , "Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.

XII. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.

XIII. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", The Journal of Systems and Software 58 , 83-91,2001.

XIV. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications,Vol-2 I 8 (2203),229-234.

XV. Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000