ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 1, January – February - 2019, Page No. 24 - 30

An Overview on Different Image Encryption Techniques

[1]Naveen Tiwari, [2]Vivek Jethani, [3]Sourabh Banga, [4]Sudhanshu Vashistha

Assistant Professor, Department of Computer Science, ACERC, Jaipur, India

Abstract

Today, the world is going to be digitized anyway. Each business unit, each government and private sector, each research unit uses the digital image as a transfer mode for all critical data. These images on the internet will not be secure. Therefore, there is a need for image security. Due to the rapid growth of digital communication and multimedia application, security becomes important issue of communication and storage of images. Encryption is one of the ways to ensure high security. The images are used in many fields, such as medical, military science. Modern cryptography provides techniques to protect information and protect multimedia data. In recent years, encryption technology has it developed rapidly and many image encryption methods were used to protect the confidential image data Unauthorized access. In this paper, different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used and also discusses the basic image security techniques or image encryption technique. The survey of the recent research in the field of image securities like Genetic Algorithm Based Approach, RSA Algorithm Based Approach, Arnold Transformation Based Approach, DCT, DFT, SVD, cryptography based approach.

Keywords: Cryptography, Decryption, Encryption, Image Encryption, RSA, Arnold Transformation

Introduction

As with the significant increase in the use of the Internet, security is an important area of concern for many applications including virtual private networks, e-commerce and secure Internet to be able to do it encryption is the art of protecting confidential information before encode or decode in illegible format and again in the legible form only by the authorized user or those who obtain the appropriate access rights. Therefore, encryption and decryption not only guarantees confidential confidentiality message, as well as integrity and prevents it from any adjustments [12].

The encryption scheme includes the asymmetric key of two uses distinctive but related keys are public and private keys password The digital image is converted into an encrypted image using the public key. This process is known as the encryption that is executed by transmitter on the other hand, the decryption of the encrypted image is they are executed taking advantage of the private key. This process is known as deciphered and executed by the receiver. Alone the recipient must know the private key. For keep your private key secret, the public key is disclosed to the public. The public key is used for authentication to make sure that the message comes from the intended sender. The public key encryption system also guarantees confidentiality. Alone the key to the receiver can decrypt the encrypted image that is being created from the sender. Messages can be made in a secure way because knowledge of the public key is not enough to decipher the encrypted image [2].

Image Encryption

With the growing growth of multimedia applications, security is a big problem in communication and storage image, encryption is a common method to maintain the security of images. Trying image encryption techniques to convert the

original image to another image is difficult to understand, to keep the image secret among the users, in other words, it is essential that nobody can know the content without the decryption process is called message Normal text encoded to encrypted text messages. Encrypted and reverse operation to convert key Text encrypted to simple text is called decrypted. To encode the image and video applications in various fields including online communications, multimedia systems, medical images, telemedicine and military communications. Colour images are transferred and stored in bulk through the Internet and wireless networks, which benefit from multimedia technologies and fast-growing networks. In recent years, many of the proposed paths to encrypt colour images so far, many data encryption proposed algorithms and use it on a large scale, such as GA or AES or RSA or IDEA, most of which are used in the text or binary data. It is difficult to use directly in multimedia data and inefficient to encrypt colour images due to the strong correlation between the pixels. For multimedia data, they are often very frequent and large and require interactions in real time. In the image or data encryption Chirp Z-Transform (CZT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Arnold Transformation is also used.

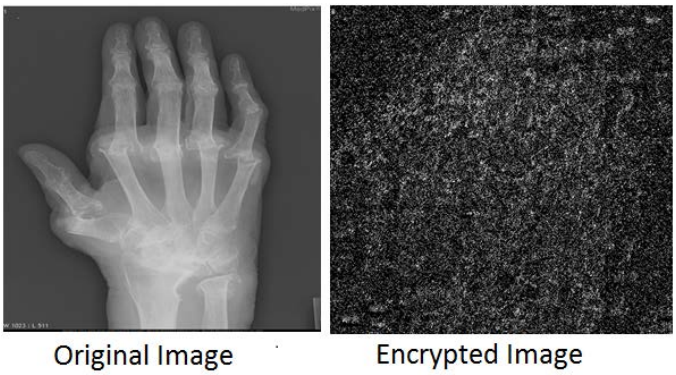

Figure 1 : Image Encryption

Cryptography

The many schemes used for enciphering constitute the area of study known as cryptography.

There are three types of cryptography:

Secret Key Cryptography

This type of encryption technology uses a key. The sender applies a key to encrypt a message while the recipient implements the same key to decrypt the message. Since only one key is used, we say that it is a symmetric encryption. The biggest problem with this technique is the distribution of keys because this algorithm uses an encryption or decryption key.

Public Key Cryptography

This type of encryption includes two key encryption systems with secure connection. It can occur between the receiver and the transmitter through a communication channel. Because a pair of keys is applied here, this technique is also known as asymmetric encryption.

In this way, each party has a private key and a public key. It does not reveal itself. The public key is shared with all the people with whom you want to communicate. If Alice wants to send a message to Bob, Alice will be encrypted with Bob's public key and Bob will be able to decrypt the message using his own key.

Hash Function

This technique does not imply any key. Instead, it uses a fixed-length hash value that is calculated based on the plain text message. The defragmentation functions are used to verify the integrity of the message to ensure that the message is not corrupted, hacked or affected by viruses. Encryption technology requires an algorithm to encrypt data. At present, when the most confidential information is stored on computers and transmitted over the Internet, we must guarantee the security of information. The image is also an important part of our information. Therefore, it is extremely important to protect our image from unauthorized access.

Image Encryption Techniques

Genetic Algorithm Based Approch

Genetic algorithms (GA) are important non-biased breeding techniques that are used in large area solution tests. Odd random sampling can be used for rapid adaptation in image processing applications. Google Analytics uses images to classify, classify, optimize, extract features and generate images. Recent research on the functioning of the genetic algorithm in Pareek and Patidar [5] has been expressed to protect the gray medical image. Encryption of this method gave important results to protect against differential attacks, entropy attacks, unusual attacks and brute force attacks. A genetic algorithm based on the image masking mechanism with image quality was described as compressible and highly assimilable in Canaan and Nasri [6]. I have a better way to embed the results of PSNR and the images for contiguous.

Genetic algorithms simulate the process of biological evolution using the survival principle of the fittest. GAS has been used for a variety of optimization problems, such as image fragmentation include the extraction of remote sensing and extraction of medicinal properties. In contrast to the traditional improvement methods, GA uses the parallel random search to arrive at the optimal solution as well they are less likely to stagnate at the local maximum. In each new generation of population it is the values of birth and fitness for all individuals are evaluated in terms of performance in the problem area. The process of selection, crossing and mutation is it is repeated until offspring are produced with an acceptable aptitude value.

RSA Algorithm Based Approch

RSA is a public key cryptographic technique to protect data attacks RSA can be used for encryption, exchange of keys (private and public key), and digital signature. RSA is designed by Ron Rivest, Adi Shamir and Leonards in 1978. At RSA nobody can encrypt the data, but for decryption it can only be made by the authenticated recipient this encryption is based on cryptographic algorithm. In this context, the application is proposed to encode and decode brain images using of the RSA algorithm, use two keys, d (private key) and e (public key), both work in pairs, for encryption and deciphered, respectively. The original image P is encrypted image C by [1]

$C = Pe \bmod n$

The encrypted image is retrieved by

P = Cd mod n

Because of symmetry in modular arithmetic, encryption

and decryption are mutual reverses and commutative.

Therefore,

P = Cd mod n = (Pe) d mod n = (Pd) e mod n

RSA is an asymmetric key cryptosystem hypothesis that it is difficult to find the large whole factors. It involves the distribution of the public and private key for the sender and receiver to encrypt and decrypt the message, respectively. RSA is a three-step process that involves the generation of keys, the message encryption and decryption of messages. The algorithm is like as Key Generation, Image Encryption and Image Decryption [2].

ANN Based Approach

The Neuronal System is a simplified biological known as one of artificial neurons, which is widely connected with wide range of elements that neurons the brain nerves handle. Networks Are Parallel Mainly Used Massively Will Distribute Analogical Abstraction and Modelling System Features SOME Nervous Human. Capture some partially provisional forces of SES calculation. Neural network will consist of such as state activation vector components, activity aggregation rule, neurons of a connectivity model, an activation rule, a signal function, a learning rule and an environment. For the ANNs the environment considers is high rate calculation.

Kishore et al. [3] I have explained significantly the security of the ANN-based image and watermark in the wavelet domain. The experiments are performed under magnetic resonance imaging (MRI), computed tomography (CT) and ultrasound imaging (US). The method is effective in Telemedicine Applicability.

Priego et al. [4] I Security System and Hyper spectral Present is Known Waterway Hywacoss As Southern Network-based Approach I in Artificial Year 2011 The method on was tested in boats and the real-time image SHIPS and provides effective validation.

Discrete Wavelet Transform (DWT) Based Approach

This is a type of sub band encoding that is found to give a quick calculation of the wavelet transform. DCT is easy to implement and optimizes the calculation time.

Mulla et al. [7] discussed the Shuffling approach to the image compression mechanism based on DWT. In this colourful image it becomes a textured image that provides image compression. The evaluation of the performance of the proposed method is analyzed with MSE, PSNR and safety probability graphs.

In Baviskar et al. [8] introduced the image fusion mechanism to improve security with the DWT sub band exchange. The method offers reduced bandwidth usage and less transmission time because it converts colour images into textured greyscale images. The image fusion technique and the compression scheme have also been explained in detail.

SVD Based Approach

This is a reliable and robust orthogonal matrix decomposition method. SVD is an attractive algebraic transformation for image processing and possesses image properties. Even SVD properties are used completely for image processing, even

more research is needed. The properties of SVDs, such as solving least squares problems, maximum energy stacking, multivariate analysis and pseudo inverse matrix, are useful for an image.

An estimate of the Gaussian noise level based on an SVD domain for images is discussed in Liu and Lin [9]. The work carried out the estimation of the noise level of the images damaged by the noise. The mechanism can be implemented in visual signals that overcome noise estimation problems. Experimental results, it has been said that the method is reliable on the wide range of visual signals.

Bhandari and Kumar [10] presented the Cuckoo search algorithm based on satellite image contrast and brightness improvement using DWT-SVD. In this case, the input image will be divided into four different standards by DWT, while the CS algorithm will be used to optimize each sub-band of DWT. Floating, the singular low threshold sub band image matrix has been obtained. The improved image of is reconstructed by IDWT. The proposed method has a significant value of PSNR.

Arnold Transformation Based Approach

We can define Arnold transformation as follows. Let (x, y) is pointing in the unit square. It move to the (x', y') by the following equation [11].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod1 \qquad \text{_____ (1)}$$

L is length of the unit square. This transformation called 2D Arnold transformation. For digital image we can define Arnold transformation as follows. Let (i, j) be pixel for square digital image $I = [I_{i,j}]_{NXN}$ its move to another pixel using the following transform [11].

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \qquad \text{_____ (2)}$$

Arnold transformation is a periodic and invertible mapping. Besides, the Arnold transformation is valid for square images only. The Arnold transformation is used to scramble the digital images and has many applications, especially in digital watermarking. Many papers estimate the Arnold transformation period as $< N^2$ .But one paper gives a linear approximation for an Arnold period as the following equation 3 as in [11]

$$T = 1.4938N + 40.8689$$

$$2 \leq N \leq 2000 \qquad \text{_____ (3)}$$

According to the Arnold transformation concept, the coding of the position space is the original position of the pixel of the image has essentially moved, if the pixel has moved farther compared to the pixels of the original image, the degree of interference is greater. Although the coding does not change the gray level of the pixels of the original image, but you can change the image of the visual effects. The coding of the image will be compared to the original image plus "chaos", which indicates that the randomization algorithm is more efficient. Therefore, its randomization function makes the pixel image a disaster. Hence we more secure our image using the Arnold Transformation.

Conclusion

In this paper we discuss the different types of the image security or image encryption techniques. According to the study of these techniques we used the hybrid of asymmetric RSA algorithm and Arnold Transformation in our proposed methodology.

The asymmetric encryption algorithm of RSA makes encryption more secure and the receiver is not too afraid to give each sender a different key to ensure communication. And another advantage of the RSA algorithm is that the RSA algorithm is difficult to decipher because it involves the factorization of prime numbers that are difficult to factor. If in one way or another, the use of permutation or attempted piracy is able to get the decryption key is almost equal to the original key. And he can go out to decipher the image by 70-80%. Then there are possibilities that I can understand about the real image (or we can say a decrypted image).

So, to solve this problem, we use another Arnold transformation technique here. According to the Arnold transformation concept, the coding of the position space is the original position of the pixel of the image has essentially moved, if the pixel has moved farther compared to the pixels of the original image, the degree of interference is greater. Although the coding does not change the gray level of the pixels of the original image, but you can change the image of the visual effects. The coding of the image will be compared to the original image plus "chaos", which indicates that the randomization algorithm is more efficient. Therefore, its randomization function makes the pixel image a disaster. This is the reason why a hacker is able to understand the real image (70-80%, before Arnold's inverse transformation). Gets the image of a problem that is very difficult to understand and hack. Another advantage of the Arnold transformation is that it uses the module operation. So if hacker has to be knowledge of number of iteration of Arnold transformation. If you are going to predict a wrong number later, make the image more complicated and confusing.

Hence we use the Arnold transformation and Asymmetric RSA algorithm in our proposed methodology.

References

1. Santhosh Kumar B J, Roshni Raj V K and Anjali Nair, " Comparative Study on AES and RSA Algorithm for Medical images", IEEE International Conference on Communication and Signal Processing, pp- 501-504, April 6-8, 2017.
2. P.V.V. Kishore, K. S. Prajwal, M. K. Mohan, and S. Koteswarao, “Medical image watermarking with ANN in wavelet domain”, In Electronics, Computing and Communication Technologies (CONECCT), 2015 IEEE International Conference, pp. 1-6, 2015.
3. B. Priego, D. Souto, F. L. Peña, and R. J. Duro, "An ANN based hyperspectral waterway control and security system", In 2011 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA) Proceedings, pp. 1-6, 2011.
4. H.R. Kanan, and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Systems with Applications, Vol. 41, No. 14, pp. 6123-6130, 2014

5. A. Mulla, J. Baviskar, S. Wagh, N. Kudu, and A. Baviskar, “Probabilistic triangular shuffling approach in DWT based image compression scheme”, In Communication, Information & Computing Technology (ICCICT), International Conference, pp. 1-6,2015
6. J. Baviskar, A. Mulla, N. Kudu, A. Parthsarathy, and A. Baviskar, “Sub-band exchange DWT based image fusion algorithm for enhanced security”, In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference, pp. 534-539, 2014
7. A.K. Bhandari, V. Soni, A. Kumar, and G. K. Singh, "Cuckoo search algorithm based satellite image contrast and brightness enhancement using DWT–SVD", ISA transactions, Vol. 53, No. 4, pp.1286-1296, 2014
8. Khalid Hamdnaalla1, Abubaker Wahaballal and Osman Wahballa1, “Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithm", International Journal of Video&Image Processing and Network Security IJVIPNS-IJENS Vol:13 No:04, pp-6-17, August 2013
9. Shikha Mathur, Deepika Gupta, Vishal Goar and Manoj Kuri, “ANALYSIS AND DESIGN OF ENHANCED RSA ALGORITHM TO IMPROVE THE SECURITY”, 3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT 2017), pp-1-5, 2017.