International Journal of Advanced Computer Technology (IJACT)
ISSN: 2319-7900 Volume VII, Issue IV, June, 2018

IMPROVED PERFORMANCE OF DIGITAL IMAGE DATA SECURE SYSTEM BASED ON HTBSC

Imroze Aslam, M. Tech. Scholar Department of CSE, RGPM, Bhopal, M.P., India; imrozeaslam1609@gmail.com
Prof. Ratan Singh Rajput, HOD, Department of CSE, RGPM, Bhopal, M.P., India, mr.ratan.proff@gmail.com

Abstract

Digital image data secure techniques have recently grows area because in this field great awareness due to secure image data or its importance for a large number of multimedia applications. Digital images data are increasingly transmitted over non-secure multimedia channels or Internet. Some important area like military, medical and quality control images data must be protected against attempts to important work. Important work could corrupt image data problem insecure important image data. To protect the authenticity of multimedia images, several approaches have been proposed. Encryption is used to transmit data securely in open networks. Information contents may be image data. Encryption of text or images, which cover the highest percentage of the multimedia, is most important during secure transmission of information. There are so many different techniques that should be used to protect confidential image data from unauthorized access. The three most important factors of image data secure design imperceptibility or undetectability, capacity, and security. As a performance measure for image distortion due to image data embedding, the well-known peak-signal-to noise ratio. It compute peak signal to noise ratio between two images, in decibels unit if image. This ratio is often used as a quality measurement between the original image data and a secure hard image data. Main parameter finds higher the PSNR, image data the better the quality of the hard or reconstructed image.

Keywords—Image Data Security, Steganography, Histogram, Visibility, Robustness, PSNR, MSE.

I. INTRODUCTION

Information had an overriding role throughout history in any respect times. Its management is similar of ability and power. It will represent battle plans, secret negotiations or current events and TV news. Exploitation of data will bring richness. Data won't to be transmitted by manuscript or by voice; currently it will travel thousands of kilometers in some tenths of second because of waves and cables. These quick technological developments create data very necessary in our life. However, this powerful data is currently additional volatile and may be simply intercepted or reproduced with all the implications that we are able to imagine like false medical diagnostic, false military targets or false proof of events [1]. The wide accessibility of powerful digital image process tools permits intensive access, manipulations and use of visual materials. In fact, lot of people might currently simply create unauthorized copies and manipulate pictures in such the simplest way that will result in huge money or human lives losses. These issues may be higher understood with an easy example. A patient with a significant health problem, discovered from medical diagnostic pictures, could eventually improve attributable to medical treatments. The medical follow-up of that patient involves the interpretation of historic pictures to guage the progression of the health problem in time. A possible false diagnosing will jeopardize the patient life, if the hold on image underwent malevolent manipulations, storage errors or compression, such the resulted distortions cannot be detected by the doctor. This is often an example wherever modifications aren't tolerated. However, in several different applications we want to tolerate some image process operations for transmission, improvement or restoration whereas we still ought to discover at a similar time any vital changes within the image content [2]. Steganography is that the art of concealing a message, image or file among another message, image or file. Steganography is used to secure the message one among the foremost needs of information activity is that the hidden data should be invisible. The utilization of steganography has several benefits and is extremely helpful in digital image process that makes them appropriate for a large type of applications. During this fashionable space, web offers nice convenience in transmittal giant amounts of information in numerous elements of the globe. However, the protection and security of long distance communication remains a difficulty. so as to unravel this downside of security and safety has LED to the development of steganography schemes. Steganography is totally different from watermarking and cryptography. The main objective of steganography is to cover the existence of the message itself that makes it tough for an observer to work out wherever precisely the message is. On the opposite hand, cryptography techniques tend to secure communications by dynamical the information into a kind so it cannot be perceive by an eavesdropper. And in watermarking emblem is additional vital than data. Steganography is that the variety of hidden communication. Planned a scheme of secret writing wherever a paper mask with holes is used. The user has to write his secret message

in such holes when inserting the mask over a blank sheet of paper. Then remove the mask to fill within the blank elements of the page and during this approach the message seems as innocuous text. During this paper, we've investigated the problems of locating the acceptable location during a given image and have obsessed the adjacent picture element distinction (APD) technique. The image quality is measured by suggests that of PSNR using MATLAB platform and compared [3, 4].

Histograms: A graphical illustration is analogous to a bar graph that organizes a bunch of information points into user-specified ranges. The bar chart condenses an information series into a simply taken visual by taking several data points and grouping them into logical ranges or bins. A bar chart could be a graphical show of information exploitation bars of various heights. The horizontal axis of the graph represents the color variations, whereas the vertical axis represents the quantity of pixels in this specific color. The bar chart compresses an information series into a simply taken visual by taking several data points and grouping them into logical ranges. It plots the amount of pixels for every tonal worth.

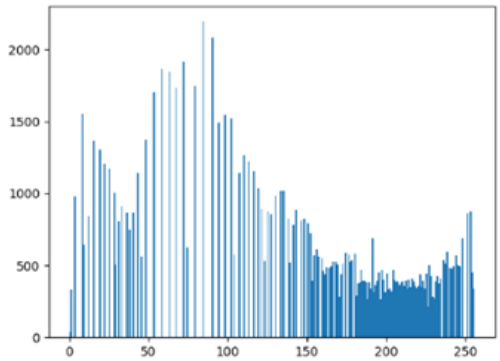

Figure 1: Histogram

Image Histogram: An image bar chart may be a graphical illustration of the pixels intensities distribution in a picture. Histograms are created from bins, every bin representing a particular intensity value vary. The bar chart is computed by examining all elements within the image and distribution every to a bin depending on the pixel intensity. The peak of a bin represents the quantity of pixels assigned to that. The quantity of bins during which the entire intensity vary is split is sometimes within the order of the root of the quantity of pixels [5].

Digital Image Content Definition Challenge

Strict image authentication considers a picture as non-authentic once simply a picture component or maybe one little bit of information has been modified. There are applications that require such service. However, this is often not the required authentication technique for many practical cases. Ideally, we want to compress a picture so as to save lots of memory space or bandwidth; we might want to reinforce a picture and restore it for higher sensory activity quality or maybe to convert its format during this context, we'd like an authentication service that tolerates specific image process operations. These image process operations modification component values while not modifying the image content.

Figure 2: image histogram

Therefore, the important drawback of selective image authentication is said to the matter of image semantic content definition. In different words, we'd like to find only changes that generate a modification within the image visual image or a mistake in its interpretation like an object disappearance or the looks of a brand new object. Consequently, to develop acceptable selective image authentication approaches, it's necessary to differentiate between manipulations that modification the image content and people that preserve it. sadly, this distinction isn't simple to comprehend technically. Moreover, this distinction may modification with pictures, applications and even at intervals one image. However, within the current literature several innovative characteristics and options are projected to explain the image content and establish content modifications. Many image process operations are listed in Tables one and a pair of. Operations given in Table one preserve image content in most cases and so authentication ways ought to tolerate them. Table two lists manipulations that modification the image content and so they need to be detected by selective authentication strategies [6]

Application Of Histogram Method

A. CT lung studies
B. Thresholding
C. Normalization
D. Normalization of images
E. Presentation of high dynamic images (IR, CT)[7]

II. LITERATURE REVIEW

Saidi A.L et al. [8].in this paper a new image encoding system utilizing fractal theories is proposed. This approach exploits the main feature of fractals generated by IFS techniques. Two levels of encryption and decryption methods performed to enhance the security of the system. The encrypted date represents the attractor generated by the IFS transformation, Collage theorem is used to find the IFS for decrypting data. The proposed method gives the possibility to hide maximum amount of data in an image that represent the attractor of the IFS without degrading its quality. Also to make the hidden data robust enough to withstand known cryptographic attacks and image processing techniques which do not change the appearance of image. The security level is high because the jointly coded images cannot be correctly reconstructed without all the required information.

Dinesh Gupta et al [9].For high security, encryption is one the way to protect the information from leakage. Many applications like military image database, medical imaging system and online personal photograph album require fast and robust security system because they are stored and transfer through network. Image encryption is conversion of image to a distorted form so that it can be secured from unauthorized users. In this paper reviews of some image encryption techniques and finally investigate two methods for image encryption. First technique is encryption of image by linear congruential generator. Random numbers are generated by prime modulo multiplicative linear congruential generator. These numbers are used as index for shuffling of rows, columns and pixels of an image. Second technique uses logistic maps to generate random number sequences. These random numbers are used as index for shuffling of rows, columns and pixels of an image. Finally we have analyzed two methods on basis of image quality parameters.

Sheng-Fu Liang et al [10], In this paper, a novel two-stage noise removal algorithm to deal with impulse noise is proposed. In the first stage, an adaptive two-level feed forward neural network (NN) with a back propagation training algorithm was applied to remove the noise cleanly and keep the uncorrupted information well. In the second stage, the fuzzy decision rules inspired by the human visual system (HVS) are proposed to classify the image pixels into human perception sensitive class and no sensitive class, and to compensate the blur of the edge and the destruction caused by the median filter. An NN is proposed to enhance the sensitive regions with higher visual quality. According to the experimental results, the proposed method is superior to conventional methods in perceptual image quality as well as the clarity and smoothness in edge region.

Jiankun Hu et al [11] proposed a novel pixel-based scrambling scheme to protect, in an efficient and secure way, the distribution of digital medical images. To provide an efficient encryption of a large volume of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an innovative way such that structural parameters of the encryption scheme have become a part of the cryptographic key. The cryptographic key of this operation is a true random number sequence generated from multi-scroll chaotic attractors. Two techniques for random number generation are discussed below.

Manjinder Kaur et al. [12] reported that Image compression is a method through which we can reduce the storage space of images, videos which will helpful to increase storage and transmission process's performance, Images are compressed using lossy and Lossless compression schemes. In this paper Fractal image compression is discussed. Fractal image compression is a lossy compression method for digital images, based on fractals. The method is best suited for textures and natural images, relying on the fact that parts of an image often resemble other parts of the same image. Fractal Encoding involves partitioning the images into Range Blocks and Domain. Blocks and each Range Block are mapped onto the Domain Blocks by using contractive transforms called the Affine Transforms. The Fractal encoding technique takes a longer encoding time and less decoding time.

G.A. Sathish Kumar et al. [13] proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. The random-like nature of chaos is effectively spread into the encrypted image through permutation and transformation of pixels in the plain image. The pixel transformation results in the encryption scheme being resistive to cryptanalytic attacks. Simulation results show high sensitivity to key, plaintext and cipher text changes. From a cryptanalytic point of view, the scheme is highly resistive to known/chosen plaintext and cipher text attacks. The proposed technique gives good parametric and sensitivity results proving itself an eligible candidate for image encryption. Moreover it is a lossless encryption technique and hence use for securing medical and military image.

Linhua Zhang et al [14] improved the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to

statistic attack, differential attack and grey code attack. In this paper implementation of spatial S-box and design of key scheme for the resistance to statistic attack and grey code attack is being done. This scheme can resist to the error function attack (EFA) which be regarded as a very effective attack recently.

Chen and Lai [15] presented security system for encryption of images using cellular automata CA by substitution of image pixels recursively. The proposed procedure performs confusion diffusion properties because of CA's flexibility. The encryption model produces lossless images using the same large secret key at both sender and receiver sides by replacing pixel values. The authors used two images color and grayscale in simulation to show strong performance. The proposed CA system uses hybrid two dimensional von Neumann cellular automata for a key stream of random sequence and recursive substitution. They also discussed the benefits of suggested system as the keys; secret, type selection, CA, and iteration keys are of variable lengths, the second benefit is that to cover replacement and cropping attack due to 2-D CA size with respect to size of image, and third one advantage is its economy in computational uses of resources for encryption and decryption as it uses only simple logical and integer arithmetic operations. And the new system is better than RC-4, AES, and 3-DES.

Verma and Jain [16] described a less complex algorithm to encrypt images using Dual Tree Complex Wavelet Transform which divide the image into approximation and detail parts. The first is encrypted with the help of pixel chaotic shuffle technique and other is protected using Arnold Transform. According to authors' claim the image is highly secured even if its first is removed without extracting algorithm then the complete image cannot be achieved. The simulation results also showed that the decrypted image at receiving end is entirely same as original while having entropy differences and mean error

III. IMPLEMENTATION AND RESULT ANALYSIS

(a) Setup Tool: Mat lab Setup tool using millions of scientist's world and engineers' use of MATLAB to analyze and design the systems. The matrix-based language of mat lab is the world's natural or easy way to graphical present express computational mathematics. Built-in graphics make it easy to visualize and gain insights from data. Mat lab setup tool using desktop environment exploration and discovery. These Mat lab Setup tool tools and capabilities are all rigorously tested and designed to work together. Mat lab Setup tool helps you take your ideas beyond the desktop. You can run your analyses on larger data sets, and scale up to clusters and clouds. Mat lab Setup tool code can be integrated with other languages, enabling you to deploy algorithms and applications within web, enterprise, and production systems. Intel Processor, 4GB memory, and Window 8 Ultimate system. Here, this method implemented and simulating on MAT LAB 2014and for this work they use Intel dual core processor 1.836 GHz Machine and operating system window-xp. The Performance analysis of MATLAB (R2014a) i.e. used for this thesis Implementation of data mining provides processor optimized libraries for fast execution and computation and performed on input cancer dataset. It uses its JIT (just in time) compilation technology to provide execution speeds that rival traditional programming languages. It can also further advantage of multi core and multiprocessor computers, MATLAB provide many multi threaded linear algebra and numerical function. These functions automatically execute on multiple computational thread in a single MATLAB (R2014b), to execute faster on multicore computers.

(b) Result Analysis: Overall performances analysis between PBHS and HTBSC technique based on image data more secure using histogram technique. Overall find more PSNR values and less MSE values proposed technique. But PBHS method find less PSNR values and more MSE values .overall best method HTBSC. Our proposed method reliable for image secure.

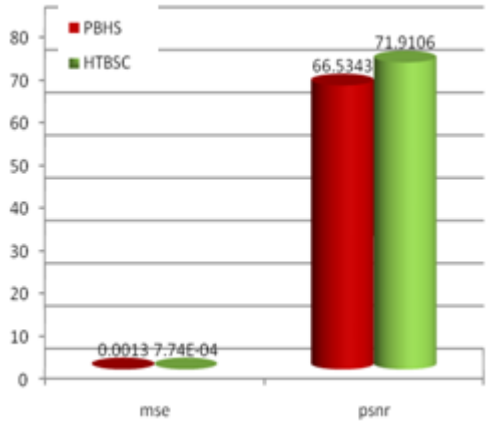

Fig 3 Performances Analysis between PBHS and HTBSC base on MSE and PSNR

VI. CONCLUSION

Various techniques involving geometry for image encoding is studied of these techniques have their own benefits and drawbacks. The utilization of fractals enhances the perplexity of the encrypted image however at a similar time it should prove to be complicated to the user itself. Pattern generation method is time consuming that could be a disadvantage to the user because the whole encoding method can become time overwhelming, however on the opposite

hand its advantageous because cryptographically attacks like brute force attack is avoided because of a similar. this can be thus as a result of it'd be a really tedious task for the attacker to guess the key since the Benoit Mandelbrot geometry is very sensitive to a moment amendment in its parameters. The techniques are classified supported PSNR values that outline the peak Signal to Noise ratio between the first plain image and therefore the encrypted image. The Mean square Error (MSE) should be most between the first image and therefore the encrypted image and therefore the PSNR should be low because PSNR is inversely dependent on the MSE.

REFERENCE

[1]. Cover TM, Thomas JA, "Elements of information theory". Wiley, New York, NY, 1991.

[2]. Dugelay J-L, Rey C Un panorama des Méthodes de Tatouage Permettant d'Assurer un Service d'Intégrité. Revue Traitement du Signal 18(4), France, 2002.

[3]. S.B. Sadkhan., "Cryptography: Current status and future trends", in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.

[4]. Y.C. Li, C.M. Yeh and C.C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility", Elsevier Journal of Digital Signal Processing, Vol. 20, pp.1116–1128, 2010.

[5]. G. A. Sathishkumar, Srinivas Ramachandran and K. Bhoopathy Bagan. "Image Encryption Using Random Pixel Permutation by Chaotic Mapping, IEEE Symposium on Computers and Informatics, 2012.

[6]. Dittmann J, Steinmetz A Content-based digital signature for motion pictures authentication and content-fragile watermarking. In: Proceedings of the IEEE international conference on multimedia computing and systems, vol II. Florence, Italy, pp 209–213, 1999.

[7]. Harpreet Kaur, Neelofar Sohi, "A Study for Applications of Histogram in Image Enhancement" The International Journal of Engineering and Science (IJES), Volume-6, Issue -6, PP 59-63, ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805, 2017.

[8]. Nadia M. G., A L-Saidi, "On the Security of Image Encoding Based on Fractal Functions", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 3 No. 1 Jan 2011.

[9]. Dinesh Gupta, Sukhjeevan Kaur, "A Review of Image Encryption Schemes Based on the Chaotic Map", Int. J. Computer Technology & Applications, Vol 5 (1), 144-149, 2014.

[10]. Sheng-Fu Liang, Shih-Mao Lu, Jyh-Yeong Chang, Member, IEEE, and Chin-Teng (CT) Lin, Fellow, IEEE, " A Novel Two-Stage Impulse Noise Removal Technique Based on Neural Networks and Fuzzy Decision ", IEEE Transactions On Fuzzy Systems, Vol. 16, NO. 4, August, 2008.

[11]. Hu, Jiankun, and Fengling Han. "A pixel-based scrambling scheme for digital medical images protection." Journal of Network and Computer Applications 32, no. 4. 2009.

[12]. Manjinder Kaur , Gaganpreet Kaur, "A Survey of Lossless and Lossy Image Compression Techniques", international Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, ISSN: 2277 128X, February 2013.

[13]. Sathishkumar, G. A., Srinivas Ramachandran, and K. Bhoopathy Bagan. "Image encryption using random pixel permutation by chaotic mapping." In Computers & Informatics Symposium on, pp. 247-251. IEEE, 2012.

[14]. Zhang, Linhua, Xiaofeng Liao, and Xuebing Wang. "An image encryption approach based on chaotic maps." Chaos, Solitons & Fractals 24, no. 3,759-765, 2005.

[15]. R. J. Chen and J. L. Lai. "Image security system using recursive cellular automata substitution", Pattern Recognition, vol. 40, pp. 1621-1631, 2007.

[16]. A. Verma, and A. Jain, "Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform", Journal of Network Communications and Emerging Technologies, Vol. 6, Issue 5, pp. 8-11, 2016.