A STUDY ON VISUAL CRYPTOGRAPHIC ENCRYPTION TECHNIQUE FOR SECURING MEDICAL IMAGES

B. Aishwarya Student , Department of IT, Dr . N.G.P Arts and Science College, Coimbatore.

Dr.V. Vinodhini , Professor, Department of IT, Dr . N.G.P Arts and Science College, Coimbatore.

N. Vanitha, Assistant Professor, Department of IT, Dr.N.G.P Arts and Science College, Coimbatore

Dr.K.Santhi, Associate Professor, Department of IT, Dr.N.G.P Arts and Science College, Coimbatore

ABSTRACT

The work "Homomorphic encryption technique for securing Medical images" is designed using image sharing mechanism by implementing cryptography function. With the help of this system one can send the images securely with his/her encryption key. So the server can't have the access on the images. The only authorized receiver with the key can decrypt the images which have been sent by the sender. Key generation is nothing but it is a symmetric key for providing security over the communication medium. Image encryption plays a paramount part to guarantee classified transmission and capacity of image over network. Then again, a real-time image encryption confronts a more noteworthy test because of vast measure of information included. This system convert's image in unreadable format using homomorphic encryption so the server cannot access the images without decryption key. So this mechanism is secured when compared to existing system. With the help this hacker can't access the data in server because the data will be in encrypted format. No one can access the data except the destination festivity/receiver.In future, we will concentrate on new inspired algorithms to enhance the execution of the homomorphism encryption.

Key words: *Visual cryptography, Encryption, Decryption, Medical images, secret sharing, Secret messages.*

1.INTRODUCTION

Visual Cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Medical images have become an essential part of medical diagnoses and treatments. The many diseases are better diagnosed through medical imaging. Occasionally, there are needs to refer patients for further diagnosis and treatment without physically moving their medical records to the referred location and these are usually transferred through network communication infrastructure such as the internet. Usually, medical images are classified information that should be treated with utmost confidentiality. Now to ensure the integrity and confidentiality of a medical image, medical professionals must properly secure these data with the network communication infrastructure in order for the patient referred location to receive the exact transferred medical image.

Nowadays the transmission of images is a daily routine, and it is necessary to find an efficient way to transmit them over the networks. With the number of internet users on the increase every day, every-thing done online is under the threat of malicious intruders. The transmission of images over the internet is challenging because of the high risk of eavesdroppers and inter-net communication hackers. In this manner, one of the secured means of transmitting the image over

the internet is cryptography. The usage of the internet for the transmission of multimedia content has become a very frequent medium for the exchange of digital information almost all institutions that are using the internet.

It is therefore important to secure data over open and unsecured networks in order to ensure safety of sensitive data. Medical information of patients are sensitive and needed to be protect during storage, especially in the cloud, and during transmission between two hospitals. Hence the usage of cryptography in the protection of such data is very crucial. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. This proposed method makes it difficult for decryption of the image without prior knowledge of the algorithm and the secret key used.

2. RESEARCH METHODOLOGY

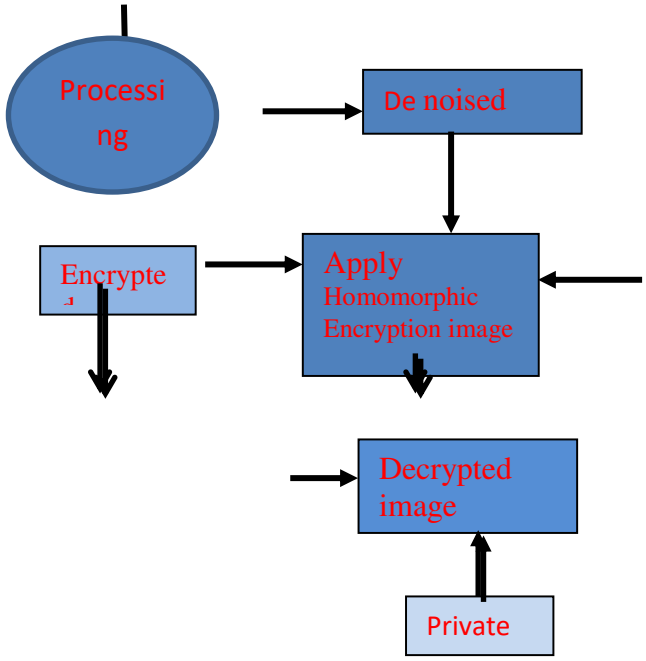

Figure 1 Methodology

3. VISUAL CRYPTOGRAPHY

Visual Cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In today's computer generation, data security, hiding and all such activities have become probably the most important aspect for most organizations. These organizations spend millions of their currency to just secure their data. This urgency has risen due to increase in cyber theft/ crime. The technology has grown so much that criminals have found multiple ways to perform cyber crime to which the concerned authorities have either less or not sufficient answer to counter. Hence, the method of

Cryptography provides the above answers. One of the most major parts of cryptography is Visual cryptography. It has many usage & application areas, mostly using its internal technique called encryption.

Figure 2 Cryptography

Visual cryptography allows for image encryption and decryption using visual technique. This technique uses an encoding and decoding scheme to protect the data privacy. By use of this technique no one accept the sender and intended receiver knows about the data transferred. A visual cryptography scheme is a kind of secret sharing scheme which allows thee encoding of a secret image into shares distributed to participants. The beauty of such as scheme is that a set of qualified participants is able to recover the secret image with out any cryptographic knowledge and computation devices. An extended visual cryptography scheme is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional.

In this work, we propose a construction of which is realized by embedding random shares into meaningful covering shares, and we call it the embedded. Experimental results compare some of the well-known proposed in recent years systematically, and show that the proposed embedded has competitive visual quality compared with many of the well-known in the literature. In addition, it has many specific advantages against these well-known, respectively.

4. ENCRYPTION

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Unencrypted data, often referred to as plain text, is encrypted using an encryption algorithm an an encryption key. This process generates cipher text that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. Today's most widely used encryption algorithms fall into two categories: symmetric and asymmetric.

5. DECRYPTION

Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. Decryption without

the correct key is very difficult, and in some cases impossible for all practical purposes.

. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

6. MEDICAL IMAGES

Medical image data is a central part of diagnostics in today's healthcare information systems. The engaged original plain image data in the cryptographic and watermarking methods should be fully recoverable due to the sensitivity of the data conveyed in medical images. A digital encryption of medical images before transmission and storage is proposed as a way to effectively provide protection of patient information. Encryption before watermarking or secret key of these images is necessary in order to ensure inaccessibility of information to unauthorized personnel with patient.

Types of medical images are

- **X-rays**
- **CT scan(computed tomography scan)**
- **MRI(magnetic resonance imaging)**

x-rays

x-rays are a form of electromagnetic radiation, similar to visible light. Unlike light, however, x-rays have higher energy and can pass through most objects, including the body. Medical x-rays are used to generate images of tissues and structures inside the body. If x-rays travelling through the body also pass through an x-ray detector on the other side of the patient, an image will be formed that represents the "shadows" formed by the objects inside the body.

Figure 3 Sample Medical Image

How do medical x-rays work?

To create a radiograph, a patient is positioned so that the part of the body being imaged is located between an x-ray source and an x-ray detector. When the machine is turned on, x-rays travel through the body and are absorbed in different amounts by different tissues, depending on the radiological density of the tissues they pass through. Radiological density is determined by both the density and the atomic number (the number of protons in an atom's nucleus) of the materials being imaged. For example, structures such as bone contain calcium, which has a higher atomic number than most tissues. Because of this property, bones readily absorb x-rays and, thus, produce high contrast on the x-ray detector. Conversely, x-rays travel more easily through less

radiologically dense tissues such as fat and muscle, as well as through air-filled cavities such as the lungs. These structures are displayed in shades of gray on a radiograph.**CT scan**A computerized tomography (**CT**) or computerized axial tomography (CAT) **scan** combines data from several X-rays to produce a detailed image of structures inside the body. **CT scans** produce 2-dimensional images of a "slice" or section of the body, but the data can also be used to construct 3-dimensional images.

MRI scan

An MRI scan uses a large magnet, radio waves, and a computer to create a detailed, cross-sectional image of internal organs and structures.

- MRI uses a strong magnetic field and radio waves to create detailed images of the organs and tissues within the body.
- Since its invention, doctors and researchers continue to refine MRI techniques to assist in medical procedures and research. The development of MRI revolutionized medicine.

Facts on MRI scanning

- MRI scanning is a non-invasive and painless procedure.

Advantages

- Advances in medical image encryption is the content protection of digital medical images is getting more importance , especially with the advance of computerized systems and communications networks which allows providing high quality images , sending and receiving such data in a real- time manner.
- The speed helps enhance the care patients receive and also improves workflow and health care efficiency
- In DICOM imaging is that physicians and other caregivers can view the images on a workstation regardless of where they are in the hospital or care facilities
- **Secret key**

Secret key is a communicating parties, user1 and user2, use same key to encrypt and decrypt the messages. …secret key cryptography is also called symmetric cryptography because the same key is used to both encrypt and decrypt the data.

7. HOMOMORPHIC ENCRYPTION

For encrypt the data or image, homomorphism encryption plays an extra operation which is denoted as a public key cryptosystem. This procedure has four functions, which are a Key generation, Encryption, Evaluation, and decryption, additionally, decrypt the information of evaluation algorithm it provides an identical out-come if we had completed the operation on the first messages The decision of the plan is subject to the sort of operations being completed

in the applications separated from different variables accustomed to pick the encryption plot.

8. KEY GENERATION

A technique for encoding and decoding keys and the related image utilizing a symmetric key; both secrecy and trustworthiness security is given. A private key and its relating public key; a key match is utilized with an asymmetric key (public key) algorithm. Presently key Generation algorithm continues to pick the extra parameters to register the public key and private Key.

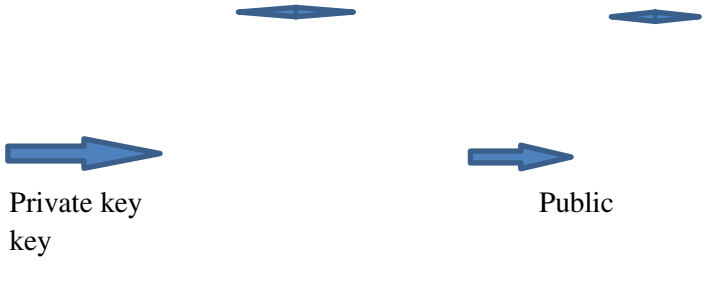

Figure 4 Key generation

In the encryption process, the images used had their RGB colours shuffled to obtain ciphered images. The ciphering of the images for this research was dependent solely on the RBG pixel values of the images and the secret key obtained from the image. There were no changes of the bit values of the images used and there was no pixel expansion at the end of the encryption and the decryption process. The numerical values of the pixels were displaced from their respective positions and the RGB values were interchanged in order to obtain the ciphered images. The characteristic sizes of image remained unchanged during the encryption process.

In this paper, the problem of pixel expansion is eliminated and also a method is proposed for colour image usage and thus the degradation of the resultant image is reduced. A secret image (secret key) is taken and is split into RGB components. Each component is handled separately.

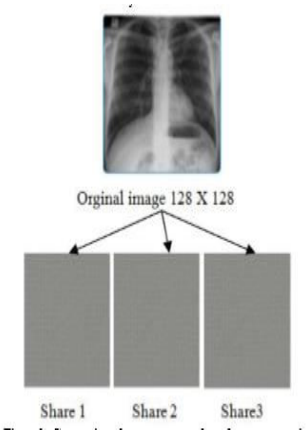

Figure 5 Generating three separate shared transparencies for gray –level visual cryptography

If the direct shares are combined a perfect gray scale image cannot be obtained. If it combines the half shares, the original quality of the image will be revealed without any loss of generality.

In this scheme, medical image is read from the dataset and extracting original pixels. Meanwhile, key matrix is randomly generated which holds the values 1 through N number of shares given by user. After that key matrix index has been noted and compared it into the same

index of original image, place it into corresponding share images and remaining values of shadow images. A software program was written to demonstrate the effectiveness of the algorithm using java programming language and cryptanalysis performed on the secret keys, Execution Time and**Formula used, Execution Time (Et)= End time** (Ete)**-Start Time**(Stte)**. Amount of** emory **Memory (M) = End Memory** (Emy) **- Start Memory** (Emy)**.**

9. HOMOMORPHIC ENCRYPTION CRYPTOGRAPHY

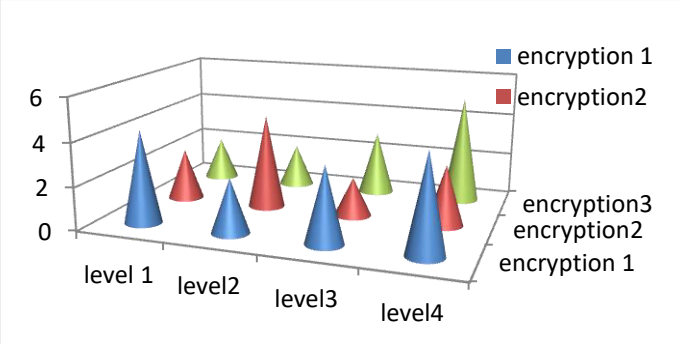

Figure 6 Encryption pie chart

9. EXPERIMENTAL RESULTS

A novel CVSS algorithm, implemented in visual studio environment is used and applied on CR and CT images the result as shown in fig.9 and fig.10 it includes original medical image, individual shares and reconstructed original images. It is used to convert and encrypt to the original images and the secret key individual share of the medical images

10.CONCLUSION AND FURURE WORK

The encryption process was effective for all the images and there was no pixel expansion at the end of the process. The entropy, mean and Sec

ret key values for the images in figure 2, figure 3 and figure 4 respectively .A slight change in the ciphered image size and pixel values resulted in a change in the decryption result**.** This makes the algorithm very effective for closely related images. The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. That is the average total pixel before encryption was the same as the average total pixel after encryption. This paper proposed a model for investigating digital Image processing operations on the encrypted images by adopting optimal key based Homomorphic Encryption. A proficient encryption algorithm that fulfills the HE to perform encryption and decryption on every one of the images is proposed. In future, we will concentrate on new inspired algorithms to enhance the execution of the homomorphism encryption. Enduring and future progression in cryptography procedures, such as, that on dynamic completely homomorphism encryption and lightweight secure correlation conventions, will be basic in making the cryptography based approach more useful for the utilization of content based image recovery.

11. REFERENCES

1) Kester, Q. A., & Danquah, P. (2012, October). A novel cryptographic key technique. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on (pp. 70-73). IEEE.
2) Mandal, J.K.; Ghatak, S., "A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography (SCOSVC)," Electronic System Design (ISED), 2011 International Symposium on , vol., no., pp.329,334, 19-21 Dec. 2011
3) M. Ali Bani Younas and A. Jattan, "Image Encryption Using BlockBased Transformation Algorithm," IAENG International Journal of Computer Science, 35:1, IJCS 35 1 03
4) M. Mohaupt and A. Hilbert, "Integration of Information Systems in Cloud Computing for Establishing a Long-term Profitable Customer Portfolio," *IAENG International Journal of Computer Science*, vol. 40, no. 2, pp. 124–133, 2013.
5) M. B. Andra, T. Ahmad and T. Usagawa, "Medical Record Protection with Improved GRDE Data Hiding Method on Audio Files," *Engineering Letters*, vol. 25, no. 2, pp.112–124, 2017.
6) V. Waghmare and S. Kapse, "Authorized Deduplication: An Approach for Secure Cloud Environment," *Procedia ComputerScience, Elsevier*, vol. 78, pp. 815–823, 2016.
7) Z. Kartit and M. El Marraki, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage," *Engineering Letters*, vol. 23, no. 4, pp. 277–282, 2015.
8) K. Brindha and N. Jeyanthi, "Secured Document Sharing Using Visual Cryptography in Cloud Data Storage," *Cybernetics andInformation Technologie,* vol. 15, no. 4, pp. 111–123, 2015.
9) K. Kaur and V. Khemchandani, "Securing Visual Cryptographic Shares Using Public Key Encryption," *in Proc. of the IEEEInternational Conference on Advance Computing Conference (IACC),* 22-23 February, 2013, Ghaziabad, India, pp. 1108–1113.
10) M. Vengadapurvaja, G. Nisha, R. Aarthy and N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security," *Procedia Computer Science, Elsevier,* vol. 115, pp. 643–650, 2017.