ISSN 2063-5346

MEDICAL DATA ENCRYPTION AND DECRYPTION USING HOMOMORPHIC TECHNIQUE

[1]Mayank Verma, [2]Dr.Ajay Kushwaha
[1]Research Scholar, [2]Professor,
[1,2]Department of CSE, Rungta College of Engineering and Technology, Bhilai, CG, India

Article History: Received: 02.04.2023 **Revised:** 20.05.2023 **Accepted:** 22.06.2023

Abstract
Encryption in cryptography is the process of encoding a message or piece of data so that only authorized parties may read it. The only thing encryption does is make it so an eavesdropper can't understand what's being said. The plaintext of a message or other piece of information is encrypted with an encryption algorithm (a cypher) to create unreadable ciphertext. A pseudo-random encryption key produced by an algorithm is typically used in an encryption system for practical reasons. It is theoretically feasible to decode the message without the key, but doing so would involve a lot of time, effort, and expertise, as well as a well-designed encryption method. If the sender includes a decryption key for the intended recipients, they will have no trouble reading the communication. In this study, we present the architecture of a system in which sensitive patient information is concealed. Radiology report digital in order to send information securely.
Key words: Encryption, ciphertext, plaintext, decrypt.

I. Introduction

As the old adage goes, a picture is worth a thousand words because it may convey more information visually than can be conveyed in words. Therefore, it is necessary to have a suitable means of visual data representation, storage, and transmission. The importance of safe data storage and transmission is rising. Images are employed in many processes because they can store more data. Visual encryption and decryption methods are vital in image data protection due to the widespread usage of digital photographs in fields as diverse as medicine, the armed forces, and private industry. Cryptography provides a method for two parties to communicate securely when in a public setting full of potential threats. The cryptographic operations of encryption and decryption take place, respectively, at the transmitter and collector closes. Encryption is the process of fusing together vital mixed-media files. files information with some additional information to transform it into the unreadable encoded "Cipher" format (known as key). Decryption is the process of converting encrypted multimedia material back into its original form using the same or a different set of supplementary information (key) [9]. Cryptanalysis is another word for the processes an attacker may employ to analyse and decode an encrypted communication channel between two parties [10]. Different cryptographic methods can be grouped together according to the guiding principles or protocols that they follow. However, in this overview, we will focus on classical cryptography and quantum cryptography. Traditional cryptography is mathematical in origin, centred on the computing challenges of factoring huge numbers. The mathematical problem of enormous number factorization

makes traditional cryptosystems safe. In addition, there are two distinct varieties of classical cryptosystems: Both asymmetric and symmetric systems However, quantum cryptography is grounded in scientific research and the principles of quantum physics. It's cutting-edge innovation that draws attention to quantum physics phenomena and makes it possible for two people to exchange information securely by exploiting the inconsistencies inherent in quantum theory. Quantum physics refers to either a numerical method or a set of notions that facilitate the development of physical theories. The Heisenberg Uncertainty Principle and the Photon Polarization Principle provide the foundation of quantum cryptography.

II. RELATED WORK

Initially, the graphic cryptography was introduced and utilised exclusively on binary graphics. Some visual cryptography systems for grayscale and colour photographs have been developed recently. In 1996, Naor and Shamir [2] introduced VCS (okay,n), the idea of a cover-based semi-bunch, to further the evaluation. Ateniese et al. [3] developed the principal VCS (2,n) with the best differentiation for every nl2. In 1997, Verheul and Tilborg [4] are fast to design a component for converting photographs to c-tones. The fundamental concept underlying this framework is to divide a single image pixel into b subpixels, with each subpixel separated into c distinct areas. Each subpixel has exactly one tinted concealment zone, whereas all other shade regions are black. The shade of one that is not completely determined by the subpixel communications. The typical variety of colours and subpixels, which is a significant hindrance to this method, leaves the nature of the discovered secret uncertain. When the number bed is large, darkening the subpixels becomes a big challenge. Tzung-Her Chen et al. [5] foresaw a multi-mystery and proposed cryptographic techniques that go beyond conventional obvious secret sharing. The codebook of conventional visual spine chiller sharing was utilised to create extent depictions full scale block by full scale block such that a few secret photographs are currently just extent photographs and translate each of the secrets individually by stacking two of percent photographs as a method of movement.

This method may be utilised for a variety of double, grayscale, and hidden images using pixel development. In [9], a hybrid system employing Watermarking and Cryptography for the transmission of a concealed text-based content message was described. This framework is mostly based on the XOR figure, the Fibonacci range, the PN range, RSA, the Hill figure, the least significant bit, no-account, and three-part Least Significant Bit. (LSB). They used Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Mean Square Error (MSE) to evaluate the quality of watermarked images. (MSE). Since MSE and RMSE were low and PSNR was strong, it was determined that the smallest bit LSB watermarking proceeded to 2-cycle LSB watermarking and 3-digit LSB watermarking. They provided variable-period input messages that were jumbled and decoded using cryptography techniques, and the encoded message was concealed using three distinct LSB watermarking algorithms. Jai Singh, Kamil Hasan, and Ravinder Kumar [10] investigated hybrid cryptographic encryption techniques and the utilisation of several encryption philosophies to enhance their level of safety and security in order to examine their combination of crossover strategies, which included the hybridization of cryptographic and digital watermarking techniques. In terms of security, the half-and-half method was shown to be less effective against programmers, and unauthorised decryption of data proved difficult. Pooja Rani and Apoorva Arora contributed to the Image Security System's use of Steganography. Regarding several photos security mechanisms. The majority

of standard photo insurance systems are not protected against the most prevalent digital attacks.

In [11], MATLAB was employed for the execution and design of the framework. Pressure was applied to reduce the size of the steganographic photograph. The undeniable truths (image) may be concealed by a chosen photograph. In the group-based steganographic approach, the real and face image insights are compared, and wherever the variety plans of the real and face images are similar, the actual image can be incorporated in those sections of the face image [11]. Discrete Cosine Conversion (DCT), Discrete Fourier Transform (DFT), and Wavelet Transform Transformation (DWT) are explored due to the comforting results obtained from their application in the field of cryptography. (grouping). The amount of time spent within the framework is calculable. PSNR and MSE have also been computed for particular limits to evaluate image quality.

III. CRYPTOGRAPHY

It is believed that cryptography arose alongside the development of writing abilities. As civilization advanced, humans were divided into tribes, clans, and kingdoms. Consequently, ideas such as power, warfare, supremacy, and politics emerged. These ideas increased people's natural need to connect in secret with a limited number of people, assuring the continuous development of encryption. The origins of cryptography may be traced back to the Roman and Egyptian civilizations. Plaintext contains sensitive information that must be kept private. It is the original text, which may include letters, numbers, executable code, graphics, or any other kind of data. Plaintext, for instance, is the text that reaches the receiver following decryption or the text transmitted in the sender's name prior to encryption.

Types of Cipher

1) Hill Cipher Method
2) Homophonic Substitution Cipher
3) Monoalphabetic Cipher
4) Ceaser Cipher

A. Hill Cipher Method

The Hill cypher is a polygraphed substitution linear algebra-based cypher that was devised in 1929 by Lester S. Hill. It was the first polygraphed cypher that it was possible to execute on more than three symbols at the time, but only just barely.

1) An encryption algorithm uses a modulo 26 integers to represent each letter of the alphabet. This basic method is utilised frequently, despite the fact that it is no longer an essential component of encryption: For the purpose of encrypting a message, an invertible n framework is utilised to improve each square of n letters. (called a n-part vector). In order to decrypt the message, each square is given a copy by the inverse of the encryption grid. The encryption lattice is the key to deciphering the code, and selecting it at random from the configuration of invertible n grids is required. (modulo 26). The code may be changed to any letters in any sequence with many letters; the mathematics just has to be performed modulo the amount of characters. This is obvious. characterised with a predisposition to modulo 26. 2) Deciphering: In order to decipher the message, we first transform the cypher text into a vector, and then we multiply this vector with the assistance of the inverse matrices of the matrix. (IFKVIVVMI in letters).

B. Homophonic Substitution Cipher

Frequency Distribution was weakened as a method of cryptanalysis by Homophonic Substitution. The first guideline of agreeable replacement is to replace the most frequently used letters with other symbols. For the letters "e" and "t," for instance, you could use six distinct images; for the letters "m" and "z," you might use two symbols each. This cypher requires a more extensive vocabulary than letters, as most letters have a preference for at least one other letter in the code text. The most typical strategy is to employ numbers within the cypher text language, although

other options include a combination of uppercase, lowercase, and inverted characters. It's not unheard of for folks to create their own unique emblems either. We'll use a key, like in the Mixed Alphabet Cipher, to keep the cypher text alphabet's characters secure. For the same reason, we use the keyword's letters first, once each time, before moving on to the rest of the alphabet. In the homophonic example, we cluster letters together and utilise more symbols to indicate the same set of 26 characters. The distribution of repeated letters after a cypher using a variety of alphabets One kind of homophonic substitution cypher is called a nomenclator. This is essentially a large homophonic substitution cypher combined with a codebook. Named after the people responsible for announcing the arrival of VIPs, the system initially consisted of a pocket-sized codebook listing the names of famous people. However, throughout time, this expanded to incorporate a great deal more general vocabulary and geographical regions. When written, the code and cypher parts are hidden from view. For a long time, many nomenclators remained uncracked because they were such a strong cypher. There are, in fact, some unbroken pieces in achieves that reveal intriguing new details about the stories they once told.

C. Monoalphabetic Cipher

Monoalphabetic cypher comes into play since both Caesar cypher and a modified version of Caesar cypher are easy to break. In monoalphabetic literature, every letter can be replaced by any other letter except the original letter. That example, A may be changed with every other letter from B to Z. You can use A, C, or Z instead of B. By passing through A, B, D, and so on, C may be changed into z. With a mono alphabetic cypher, it is hard to figure out the message since there are many substitutes and a wide variety of permutations and combinations. In a monoalphabetic encryption, each image in plain text is given a single, fixed value. One person in the visible text is the same person as one person in the encrypted communication. Each alphanumeric char in plain text is the same as a certain alphabetic char in encrypted text. A circulation cypher is monoalphabetic if the key cost doesn't change dependent on where the seen text-based man or woman is in the seen text-based flow into. It's a simple way to encrypt data that's easy to comprehend and use. There are 26 keys that might work. Because of this, the brute-force attack worked here. A Get the two mixed up Cipher is a type of encryption that uses the same static mapping from real letters to cypher letters throughout the whole document.

D. Ceaser Cipher

It is a replacement cypher, which means that every letter of the alphabet is substituted with a letter located a particular no. of places down the alphabet. A ceaser encryption is also known as a ceaser's cipher, the shift cypher, ceaser's code, or ceaser shift in cryptography. It is one of the simplest and most extensively used encryption methods. The amount of od letters used it to move the cypher alphabets defines Caesar cyphers.

Encryption Alternatively, the encryption algo may be stated using arithmetic by first converting the letters into integers, as in A 0, B 1..., Z 25. Encryption of a letter x by a shift n may be expressed mathematically as, Mod 26 * Encryption(x)=(x+n)

Decryption Caesar's code

Decryption change one letter with another an reverse alphabet: a previous message in the alphabet.

IV. PROPOSED WORK

The Cryptographic algorithm is used for encryption and decryption in this case. We use watermarking on the picture for security reasons. PyCharm programmed is being used for results and simulation. Figure 1 depicts the entire procedure.

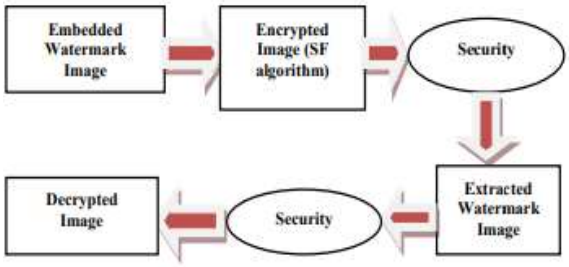

Fig.1: Process of the cryptography

Figures 2 and 3 provide a brief overview of the new encryption and decryption/recovery mechanisms. The figures represent the key created by the aforementioned procedure.

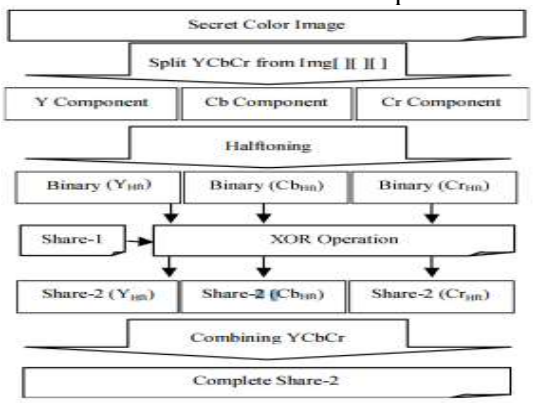

Fig. 2. Flow of encryption technique

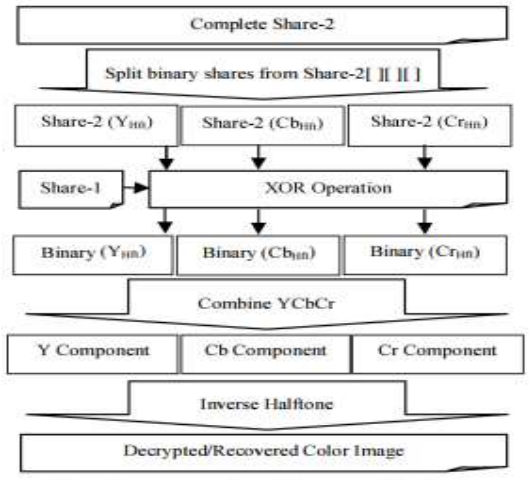

Fig. 3. Flow of decryption technique

EXPERIMENT RESULTS

We used Python software to apply our proposed technique on xray image data in this investigation. The algorithm process was used to implement our strategy. Using these approaches, we evaluated a decrypted image that was considered to be a close match to the captured photograph. The original Xray image is shown in Figure 6. After then, the original photograph was watermarked. The watermarking procedure covered all three steps of embedding, attacks, and extraction. The image with integrated text is seen in Figure 7. The method was then used to encrypt and decode data. The encrypted and decrypted pictures of the patent Xray embedded picture are shown in Figure 8.

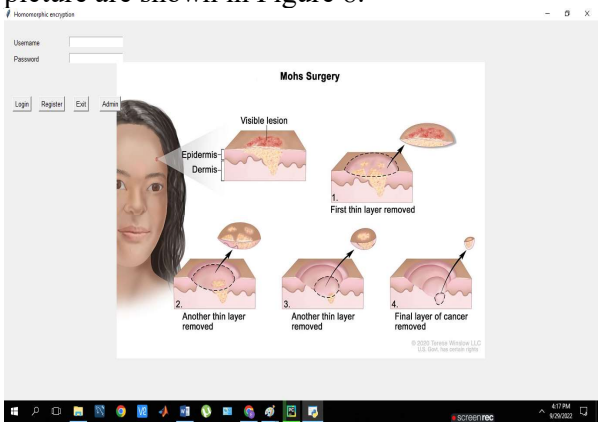

Fig 4 front panel of the system

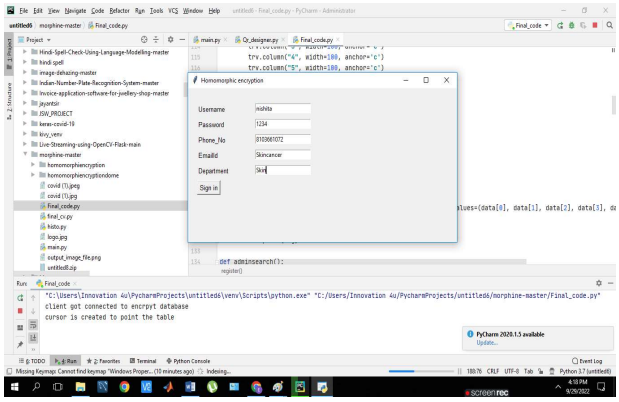

Fig 5 data Entry panel

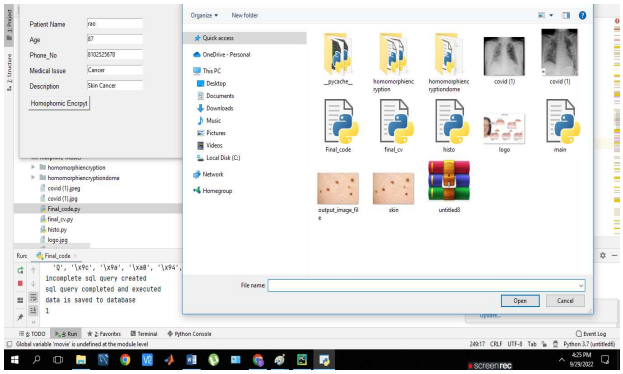

Fig 6 Xray image of Patient

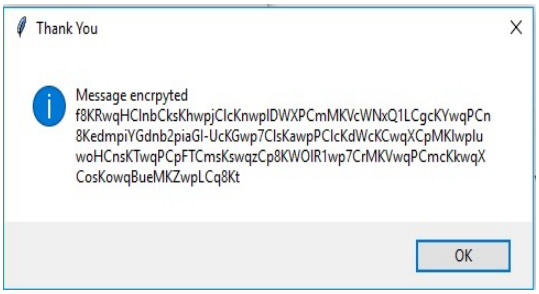

Fig 7 Encrypt text

Fig 8 Top one Input Image, Bottom One Encrypted image

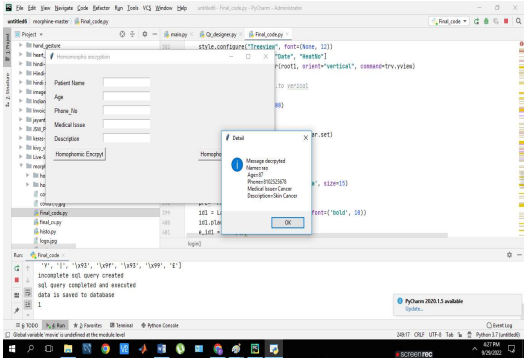

Fig 9 Decrypt Message

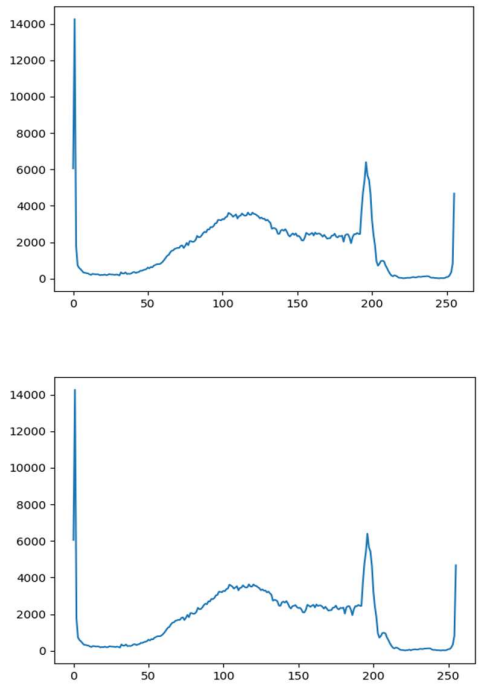

Fig 10 Histogram graph of input and after encrypted image

CONCLUSION

We presented a medical data encryption solution based on natural image cryptography in this study. This unique approach efficiently calculates key and cypher generation. The fundamental passkey image and cypher picture use up less space than the original encrypt image. Throughout the operation, the pixel of the picture stayed intact. The picture appearance of the recovered image is excellent after this operation. It might be converted to operate for identification image-based encryption due to its resilience to a restricted number of cryptographic attacks.

REFERENCESS

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology - EUROCRYPT'94, A. D. Santis., Ed., vol. 950. SpringerVerlag, 1995, pp. 1-12.

[2] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary versionappears in "Security Protocols", M.

Lomas ed. Vol. 1189 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1997, pp.197-202.
[3] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416-428.
[4] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2), pp.179-196, 1997.
[5] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, lEICE, 2008
[6] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, 2008, pp. 252-256.
[7] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.
[8] Zhengxin Fu, Bin Yu, "Research On Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, 2009, pp 533-536.
[9]. Amandeep Kaur and Satveer Singh, “A hybrid technique of cryptography and watermarking for data encryption and decryption”, IEEE, Punjab, India, 2016.
[10]. Jai Singh, Kamil Hasan and Ravinder Kumar, “Enhance security for image encryption and decryption by Appling hybrid techniques using MATLAB”, IJIRCCE, vol.3, issue 7, July 2015.
[11]. Pooja Rani and Apoorva Arora, “Image security system using encryption and steganography”, IJIRSET, vol.4, issue 6, June, 2015.