International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

ENCRYPTION AND DECRYPTION USING CRYPTOGRAPHY FOR MEDICAL DATA SECURITY

Gunna Yogesh[1] Mtech Scholar[1]

Vivek Shukla[2] Assistant Professor[2]

Dr. Rohit Miri[3] Head Of Department[3]

Department of Computer Science, Dr. C.V.Raman University Kota, Bilaspur Chhattisgarh

Abstract - In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients. In this paper we are designing a system in which we hiding patient details in there digital x-ray report For secured data transmissions.

KeyWords: encryption, ciphertext, plaintext, decrypt

I. INTRODUCTION

As the expression goes, "a picture is worth a thousand words," since it may include more graphical information than information obtained from a text for human interpretation. As a result, the representation, storage, and transmission of visual data must all be acceptable. Data storage and transmission security is becoming increasingly critical. Images are used in a number of procedures since they may hold a lot more information. Because digital pictures are used in a wide range of industries, including health, the military, and private organizations, the security of these contents is crucial, which is why visual cryptography and decryption methods are so important in image data protection. Cryptography is a means of ensuring secure communication between two groups in a public space crowded with unauthorized visitors and malicious attackers Encryption and decoding are two cryptography techniques that occur at the transmitter and collector closes, respectively. The technique of merging crucial mixed media is known as encryption. files data with some extra data in order to convert it into the "Cipher" format, which is an unreadable encoded format (known as key). Decryption is the inverse of encryption in that it decodes the cypher and transforms it to the real multimedia data using the same or a different additional data (key) [9]. Another term is cryptanalysis, which refers to the procedures that an intruder might use to examine and decrypt an encrypted message between two parties [10]. Approaches to cryptography can be categorized based on their underlying principles or protocols. However, we will concentrate on two types of cryptographic algorithms in this survey: conventional and quantum cryptography. Classical cryptography is based on the computational difficulties of factoring large numbers and is mathematical in nature. Traditional cryptosystems are secure because the mathematical issue of huge number factorization is extremely difficult. Furthermore, there are two types of classical cryptosystems: Systems that are asymmetric and symmetric Quantum cryptography, on the other hand, is science-based and is based on quantum physics laws. It's a novel technology that highlights quantum physics phenomena, allowing two individuals to safely communicate using quantum theory principles' invariabilities. Quantum physics is a numerical technique or collection of concepts that allows

physical theories to be built. Quantum cryptography is based on two key principles of quantum physics: the Photon Polarization Principle and the Heisenberg Uncertainty Principle.

II. RELATED WORK

The photograph cryptography changed into initially presented and used best on binary snap shots. Recently, a few visible cryptography schemes for gray and shade image were proposed.

In 1996, Naor and Shamir [2] provided VCS (ok,n), the thought of a cowl-based totally semi-bunch, to additionally paintings on the appraisal. Ateniese et al. [3] made the primary VCS (2,n) with the most best differentiation for each nl2. In 1997, Verheul and Tilborg [4] are quick to put out a thriller supplying issue for pics to c tones. The critical thought in the back of this framework is to partition one picture pixel into b subpixels, with each subpixel remoted into c range regions. Each sub-pixel has precisely one hued conceal area, while any closing shade regions are darkish. The color of 1 now not totally set in stone via the communications of the stacked sub-pixels. The nature of the found secret still up within the air by means of the normal range of shades and subpixels, that is a important obstacle of this system. Whenever the range bed is substantial, shading the sub-pixels becomes a considerable problem. Tzung-Her Chen et al [5] expected a multi-mystery and methods cryptographic strategies that goes past normal obvious secret sharing. The codebook of conventional visual backbone chiller sharing utilized to create quantity depictions complete scale block through full scale block all collectively that more than one mystery images are presently simply quantity pictures and translate each one of the secrets in my view by means of stacking of percentage snap shots in a way of shifting.

This technique is probably used for diverse double, grayscale, and disguise mystery snap shots with pixel improvement. In [9], a go breed arrangement the usage of Watermarking and Cryptography turned into portrayed for the conveyance of a covered textual content primarily based content message. This framework is essentially founded on the XOR parent, the Fibonacci collection, the PN collection, RSA, the Hill determine, the slightest bit, no-account, and three piece Least Significant Bit (LSB). They applied the ideas of Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Mean Square Error (MSE) to assess the exceptionality of watermarked pics (MSE). It turned into discovered that the slightest bit LSB watermarking endured to two-cycle LSB watermarking and 3-digit LSB watermarking considering MSE and RMSE have been low and PSNR was high. They gave variable-length input messages that had been scrambled and decoded using cryptography methods, and the encoded message changed into masked utilising three unmistakable LSB watermarking tactics. Jai Singh, Kamil Hasan, and Ravinder Kumar [10] explored go breed cryptographic encryption procedures in addition to the usage of some encryption philosophies to paintings on their degree of protection and safety to observe their mixture of crossover techniques, which enveloped the mixture of cryptographic and virtual watermarking techniques. As some distance as security, the half and half method changed into validated to be greater helpless towards programmers and illegal unscrambling of information became difficult. Pooja Rani and Apoorva Arora contributed the utilization of Steganography for Image Security System. For more than one image protection systems. A big part of the common photo coverage structures are not date's area to watch contrary to the least digital attacks.

In [11] MATLAB became utilized for The framework's execution and design To decrease the size of the steganographic photograph, pressure become applied. The plain realities (photograph) can be disguised at the back of a selective photograph. The authentic and face picture insights are checked in the group based steganographic technique, and any area the variety plans of the real and face photograph are comparative, the actual photo may be embedded in those pieces of the face picture [11]. Due to the reassuring results acquired from their usage within the area of cryptography, the pinnacle pressure calculations investigated here are Discrete Cosine Conversion (DCT), Discrete Fourier Transform (DFT), and Wavelet Transform Transformation (DWT) (grouping). The time frame spent in the framework can be decided. PSNR and MSE have moreover been determined for specific barriers to assess photograph fine.

III. CRYPTOGRAPHY

Cryptography is meant to have advanced alongside the development of writing abilities. Humans have been organised into tribes, clans, and kingdoms as civilization progressed. As a end result, ideas like power, battle, dominance, and politics commenced to emerge. These ideals inspired humans's herbal desire to interact secretly with a small institution of people, ensuring encryption's endured progress. Cryptography can be traced all the way lower back to the Roman and Egyptian civilizations. Plaintext is data that must be stored personal. It is the unique textual content, which may also include letters, numbers, executable programming, pix, or any other type of records. Plaintext, for instance, is the textual content that reaches the recipient after decryption or the transmission of a message in the sender's call before encryption. Types of Cipher

1) Hill Cipher Method

2) Homophonic Substitution Cipher

3) Monoalphabetic Cipher

4) Ceaser Cipher

A. Hill Cipher Method

The Hill cipher is a polygraphed substitution linear algebra-based cypher Lester S. Hill invented it in 1929, and it became the primary polygraphed cypher that was feasible (albeit slightly) to carry out on more than three symbols at the time.

1) Encryption: A modulo 26 integers is used to represent every letter. Though it's miles no longer a important characteristic of encryption, this straightforward technique is nevertheless broadly used: An invertible n framework is used to beautify each rectangular of n characters to scramble a message (known as a n-component vector). To decrypt the message, every rectangular is replicated by way of the encryption grid's inverse. The encryption lattice is the coding secret, and it must be selected at random from the arrangement of invertible n grids (modulo 26). Obviously, the code may be changed to any letters in any collection with many letters; the arithmetic simplest needs to be achieved modulo the wide variety of characters. With tendency to modulo 26. 2) Deciphering: To decode the message, we convert the cypher text into a vector and multiply this with the aid of the inverse matrices of the matrix (IFKVIVVMI in letters).

B. Homophonic Substitution Cipher

Because of Homophonic Substitution, Frequency Distribution have become a much less effective cryptanalysis device. The fundamental rule of agreeably substitution is to assign a letter or photo to the excessive frequency letters. You could, as an instance, use six exceptional photos to deal with "e" and "t," symptoms to deal with "m," and one signal to cope with "z." Clearly, this encryption will need a bigger jargon than letters, as every letter prefers at the least one code textual content letter, and plenty of like more. The maximum common technique is to include numerals inside the cypher textual content language, but you may also use a mix of capital, lower, and incorrect manner up letters. Some human beings even construct their personal customized symbols to apply. To maintain the characters of the cipher - text alphabet, we are able to appoint a key of some form, just like the Mixed Alphabet Cipher. Similarly, we employ the letters from the keyword first, and not using a repetitions, accompanied with the aid of the relaxation of the alphabet. We use significantly more letter clumping within the homophonic instance, in addition to greater symbols to represent the 26 letters. The letter frequencies following a Cipher with Mixed Alphabets A nomenclator is a sort of homophonic substitution cypher. This is a combination of a codebook and a huge homophonic substitution cypher. It turned into referred to as after the people who notified the presence of dignitaries and started with a bit codebook containing the names of celebrities. This, but, quick grew to encompass numerous common phrases, terms, and places. The code and cypher components are not seen whilst written. Nomenclators have been a totally powerful cypher, and many of them had stayed unbroken for many years. In truth, there are some portions in achieves which have not been damaged and offer charming insights into past testimonies.

C. Monoalphabetic Cipher

Because Caesar cypher and a adapted version of Caesar cypher are without problems damaged, monoalphabetic cypher enters the image. In monoalphabetic literature, any alphabet can be substituted with the help of any other alphabet shop the authentic alphabet. That is, each other letter from B to Z can be used to replace A. B can be substituted through A, C, or Z. C may be converted to z by means of going via A, B, and D, and so forth. Because there are a couple of substitutions and a super range of permutation and combination, it is hard to decipher the message the usage of a mono alphabetic cypher. A monoalphabetic encryption is one in which each photo in simple text is assigned a difficult and rapid cost. The relationship between a person in the visible text and a human within the encrypted message is one-to-one. Each alphanumeric char of undeniable text corresponds to a unique alphabetic character of encrypted textual cloth. If the important thing value does not depend upon the area of the visible text - primarily based person in the visible textual content - primarily based flow into, the circulate cypher is monoalphabetic. It is a sincere encryption approach that is easy to apprehend and execute. We have a complete of 26 possible keys. As a end result, the brute-pressure attack observed paintings right right here. A Confuse the two Cipher is an encryption method that employs the same static mapping from legitimate textual content to cipher letters all through the textual content.

D. Ceaser Cipher

It is a substitute cypher, because of this that every letter of the alphabet is substituted with a letter located a specific no. Of places down the alphabet. A ceaser encryption is also referred to as a ceaser's cipher, the shift cypher, ceaser's code, or ceaser shift in cryptography. It is one of the most effective and maximum considerably used encryption techniques. The amount of od letters used it to transport 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 ALGORITHM

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.

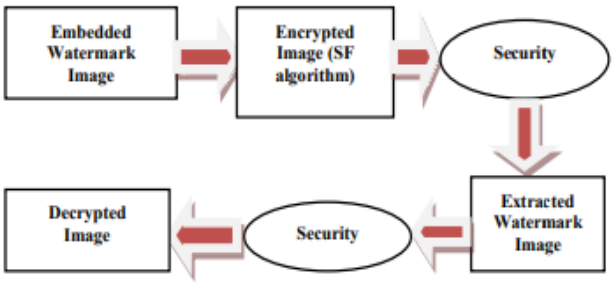

Fig.1: Process of the cryptography

V. ENCRYPTION 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.

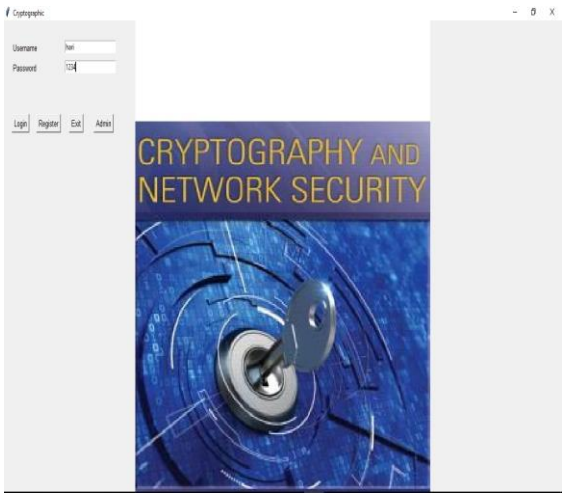

Fig 4 front panel of the system

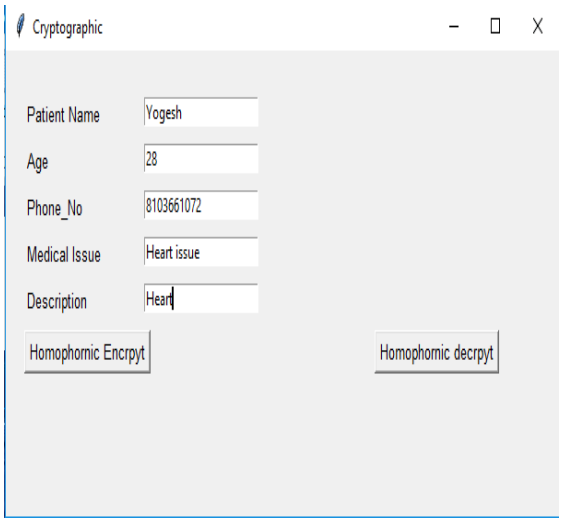

Fig 5 data Entry panel

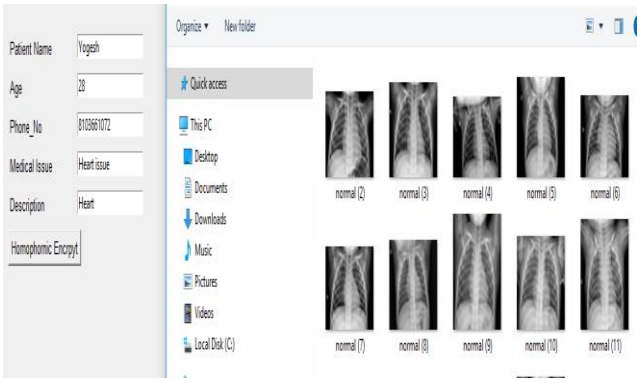

Fig 6 Xray image of Patient

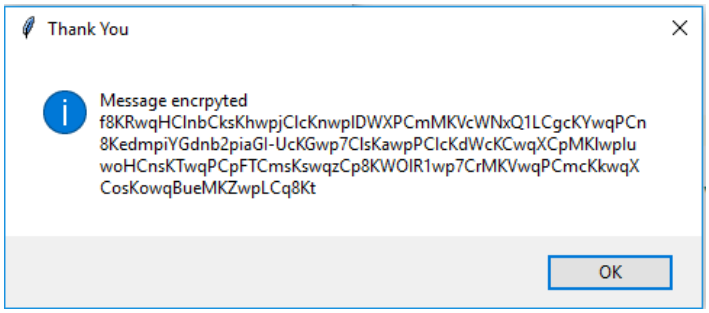

Fig 7 Encrypt text

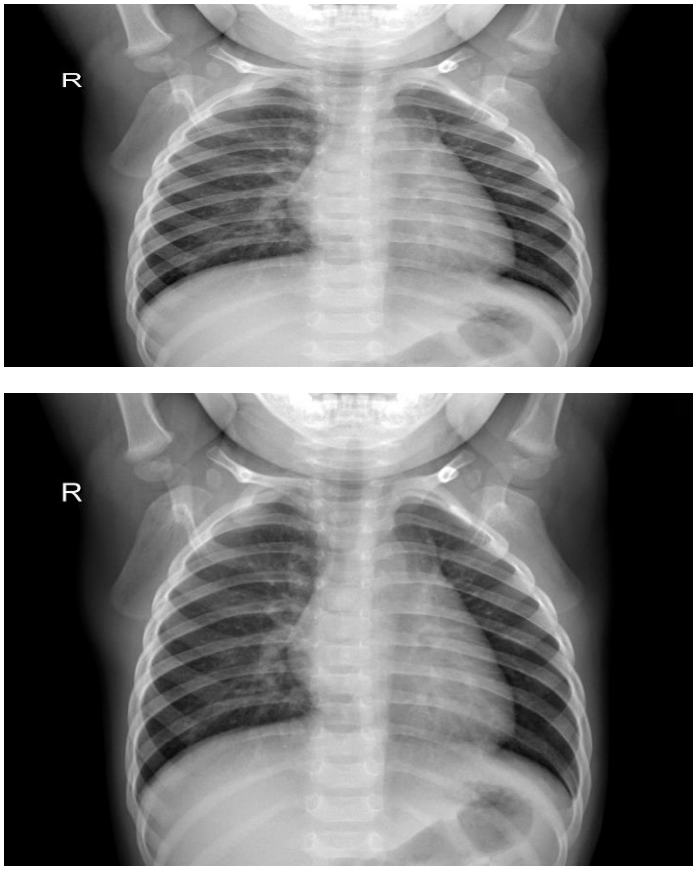

Fig 8 Top one Input Image, Bottom One Encrypted image

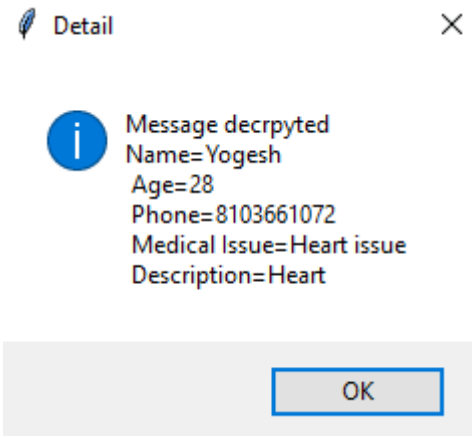

Fig 9 Decrypt Message

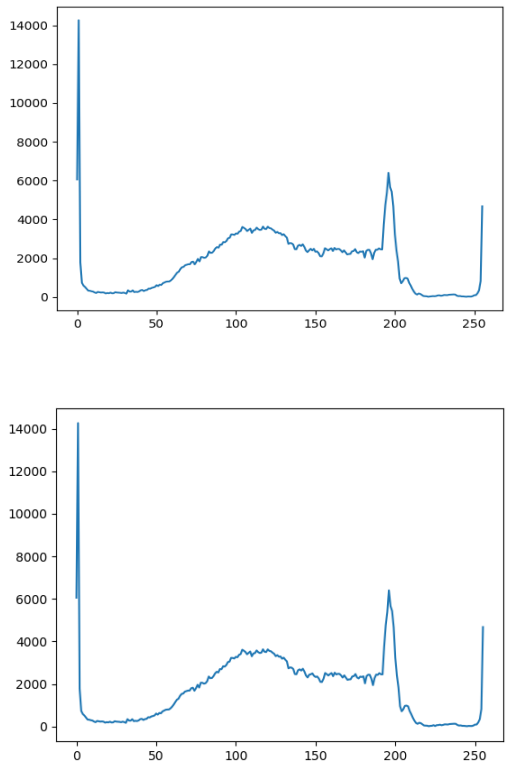

Fig 10 Histogram graph of input and after encrypted image

VI. 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.