Multimodal Biometric Image Security using Steganography and Watermarking

Sonali Kesharwani[1] Dr. Neelesh Mehra[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Samrat Ashok Technological Institute, Vidisha, Madhya Pradesh, India

Abstract— Data hiding is the key factor in secure communication today, Because of duplication and data manipulation. With the help of data hiding, that we can make our personal and important data will ensure against activities without authentication. Due to the availability of low-cost editing tools, any user can easily copy, modify, and retransmit digital data over the network. It could also cause a social disorder if digital media content, such as confidential government documents, court evidence or other important information, is maliciously manipulated. To effectively support the growth of multimedia communications, it is essential to develop tools that protect and authenticate digital information. Steganography, watermarking and cryptography of such types of methods are used to hide data in secret communications. In this proposed work use a lossless data hiding technique using watermarking and steganography together, so that achieve high security that provides a higher level of security and authentication of data without loss. Combination of watermarking and steganography techniques used to get multiple layers for hiding personal information. With the help of watermarking algorithm we are embedding the user personal information within the image. The embedding and detection method of the watermark technique used the DWT transformation. Watermarked image and secret image hide within the original cover image through steganography. The most Common use of steganography is to hide a file in another file. Discrete Wavelet Transform (DWT) method is used to obtain frequency domain analysis of the image.

Key words: Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Least Significant Bit (LSB)

I. Introduction

Data security is the practice of keeping data protected against corruption and unauthorized access. Behind data security approach is to ensure privacy at the same time protecting personal or important data. Data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy and legal issues. Data privacy issues can arise from a wide range of sources such as health records, investigations, and procedures of criminal justice, financial institutions and transactions, biological traits, residence and records geographical and ethnicity. Biometric recognition refers to the use of distinctive physiological features (fingerprint, face, retina, geometry of the hand, iris, etc.) and behavioral (vocals, step, signature, etc.), called identifiers biometric or simply biometrics.

Examples of these applications: control of physical access to a secure facility, e-commerce, access to support networks of brand etc. Traditional methods to establish the identity of the person (for example, passwords) based on the knowledge and tokens (for example, ID cards)-mechanisms based on. A biometric system is essentially a model of recognition system that works through the acquisition of biometric data of a person, extract a set of characteristics of the collected data and comparing this function to the model based on the data. Depending on the application environment, a biometric system can operate in mode identification or verification. Until the system can be put in verification or identification mode, create a database of biometric templates via the registration system. Registration is the process where the initial user biometric samples are collected, evaluated, treated and stored for use continuously in a biometric system of recognition of the biometric system provides two main features verification and identification. In failure, also called authentication, the user indicates the identity and the system verifies whether the claim is authentic. If the user input and the model of the claimed identity have a high degree of similarity, the claim is accepted as 'true '. Otherwise, the request is rejected and the user is considered to be the 'fraud '. In identification, user input is compared with models of all users registered in the standard database and the identity of the person whose model has the highest degree of similarity with user input is displayed by the biometric system. A user can be identified or checked on the basis of: (i) something you know: for example, a password, PIN etc. (ii) something: for example, a credit card, a key or a passport (iii) something that is (biometrics) : for example, a fingerprint face, iris etc using something that we and hold are two solutions identification and easy verification widely used these days. Using what we know requires only a good memory, but sometimes it can be guessed easily. Biometrics is the only thing that does not need to be recalled or performed. Security data or privacy of data has become increasingly important as more and more systems are connected to the Internet. There are laws on the protection of data or personal information of voluntary or involuntary, or inappropriate disclosure. So, hide the data in some sort of shape in an image, as it is essential to ensure that the security or confidentiality of the data.

A. Contributions and Goals

In this article, propose a framework of several layers that increases the safety of multimodal biometric data using a combination of watermarks and steganography. First, use a technique of watermark to hide using the information of the user in the cover image, once using a technique of steganography for security system dislocated multi-layer to hide the watermark and secret image. Signal-to-noise ratio (PSNR) is used to measure the quality of the reception of the image.

B. Paper Organization

The rest of the paper is as follows. Section 2 describes the work in the field while section 3 describes the methodology used. Section 4 describes the experiences that have been carried out 5 results, while section 6 provides conclusions and future work.

II. Literature Survey

Cameron Whitelam, Nnamdi Osia and Thirimachos Bourlai [1] proposed a multi-layer framework that enhances the security of multimodal biometric data using a combination of watermarking and steganography. It uses a watermark technique to hide faces in images of fingerprints fingerprints Eigen functions. After that, he used a technique of steganography to hide data as a result of the footprint or the face on an arbitrary of any significance to the biometrics or forensic image watermarked. Recessed mounting locations are set randomly in all 3 colors of arbitrary image channels.

According to Anil K. Jain and Umut Uludag [2] Biometrics-Based personal identification techniques used, Digital watermarking techniques can be used to incorporate sensitive information like the logo of the company on the host data to protect the rights of intellectual property of the data. They are also used for authentication of multimedia data. Encryption can be applied to the biometric templates to enhance security model which can be in 1) a database, 2) a brand like the smart card or 3) a biometric device such as a mobile phone with fingerprint sensor) can be encrypted after registration. Then, during authentication, encrypted templates can be read and used to generate the result corresponding with biometric data online. As encryption models are provided may not be used or modified without decryption with the appropriate key.

According to Prabha jot Kour [3], Discrete Wavelet Transform is a useful and effective tool for signal and image processing. The DWT transmits a signal to the image, throughout a pair of filters, a high-pass filter (HPF) and a low-pass filter (LPF). The low-pass filter obtains a low-resolution signal. The filter signals the difference. The original signal is reproduced when the sampled output to the LPF is added to the sampled output to the filter. The output of the HPF is fed into another filter pair and the process is repeated. The Haar wavelet transformation is the simple example of the discrete wavelet transform. The wavelet transform (WT) has largely accepted signal processing and image compression. Due to its multi-resolution nature, wavelet coding schemes are suitable for applications where scalability and degradation are important. Recently, the JPEG committee released its new standard image coding, JPEG-2000, based on DWT.

Mayank Vatsa, Richa Singh, P. Mitra [4], proposed two levels of security to check any individual and at the same time protect the biometric template. A biometric template that is watermarked iris on the face, the verification of the face is visible and the iris with watermark is used to cross authenticate the person and the protection of biometric (face), as well. To build the model iris watermark data, i.e. an algorithm based on log on1D Gabor used. 1 Dlog Gabor is being convolved with the texture of the transformed iris image, and so the model is generated. This model is called iris code. This iris code is in binary form and is unique for each individual. It is now integrated in the image of the face of the same person to protect the face model, as well as the functioning of the multimodal offers two levels of security to check any person and at the same time protect the biometric template. A biometric template that is iris watermarked in the face, the face for verification and diaphragm with water is used to cross to authenticate the person and the protection of the biometric (face).

III. Methodology

- Study of the literature will be to collect the facts and inform the contribution in this area.
- Steganography and watermarks brings a variety of very important techniques how hide important information of user. Steganography and watermarks are the main parts of the area of rapid development of having hidden information. Hence combination of these two techniques made of two layers of security. Image security is the biggest concern for the technology of the internet because of duplication and the manipulation of the original image. So we can use digital watermarks to hide personal information like Aadhaar card number, ATM PIN, fingerprint, Date of birth, etc.
- Design and development of system to protect the database of models against imposter attack using multimodal security system. Multiple data masking with at the cover image for more security we apply the method to steganography.
- Design and development of a framework of multi layers watermarking system combine with steganography system.
- If we want to apply more security for secret image apply encryption to encrypt information and hide secret image by applying an XOR of its bits operation completely.

IV. Proposed Work

Proposed algorithm uses three layers of security to maintain the accuracy of the data, privacy and the protection of personal information. First layer of security performs technical watermarks to hide personal information of the user, any data that we consider may be a fact of the text (ATM Pin, cards of Aadhaar, date of birth) or can be an image (impression of) image retinal fingers, DNA,). Second layer is applied to encrypt the secret image using encryption and the third layer to hide the image with watermark and image secret in the coverage through the image steganography algorithm.

A. Embedding Algorithm

- Input the Cover Image and calculate the size of the Cover Image.
- Input the user information (Finger print, Dna Image) and calculate the size.
- Apply Haar wavelet transform to decompose the cover image.
- User information is hide within the Cover Image by apply Watermarking Algorithm and obtained a Watermarked Image.
- Input the Secret Image and calculate the size of the Secret Image.
- Apply the Encryption in the Secret Image and obtain encrypted image by apply XOR operation.

- Load the key Information called private key.
- Secret Image and Watermarked Image are hide within the Cover Image by apply Steganography Algorithm.
- To obtain Transform (Frequency) Domain analysis apply DWT method.
- Apply IDWT Stego Image obtained.

B. *Extraction Algorithm*

- Input the Stego Image.
- Apply Haar wavelet transform to decompose the Stego image.
- Load the key Information, this key is same as private key which is enter in the embedding algorithm of steganography.
- By clicking the Extract button extract all the images which is hide in steganography process .All this process is loss less.
- Extract original cover image, secret image, watermarked image, user information.
- Calculate Peak signal to noise ratio (PSNR), Mean Square Error (MSE).

Watermarking process uses the Discrete Wavelet Transformation method. We apply here is Haar DWT. In Haar DWT low frequency wavelet coefficient are generated by averaging the values of two pixels and coefficients of high frequency are generated by one-half of the difference of the two pixels. Once the user login in the system, user can use the information along with the secret key to hide secret data within the chosen cover image. An algorithm of steganography using novel, secret information will be embedded and hidden within the cover image with almost zero distortion. To recover the information, a secret key is required. Without the secret key, the data cannot be extracted from the image. For the algorithm of steganography, the Flow chart shows the algorithm to integrate the secret message inside the cover image. Transform domain steganography method is applied in our work. Haar wavelet transformation method is applied for the frequency domain image analysis. The secret key is used for the verification process to retrieve the correct information from the image. The data extracting method, a secret key is needed, to detect whether the user enter the right key or not a message box is display. If key is not match then key is mismatch message is display and message shows please enter the right key. Once the key is matched, the process is continues this secret key is also embedded together with the data inside the cover image. Therefore, when a user transmits the image over the internet, it contains data and password, as well. However, data can only be obtained from the image using the system. The extraction process used to reverse the process of embedding. When a stego object is sent to the extraction process, the elements of the stego are arranged in the same sequence as the process of embedding. Reconstruction of the embedding method has access to the key k used in the process of embedding. The PSNR and MSE value are calculated to analyze result.

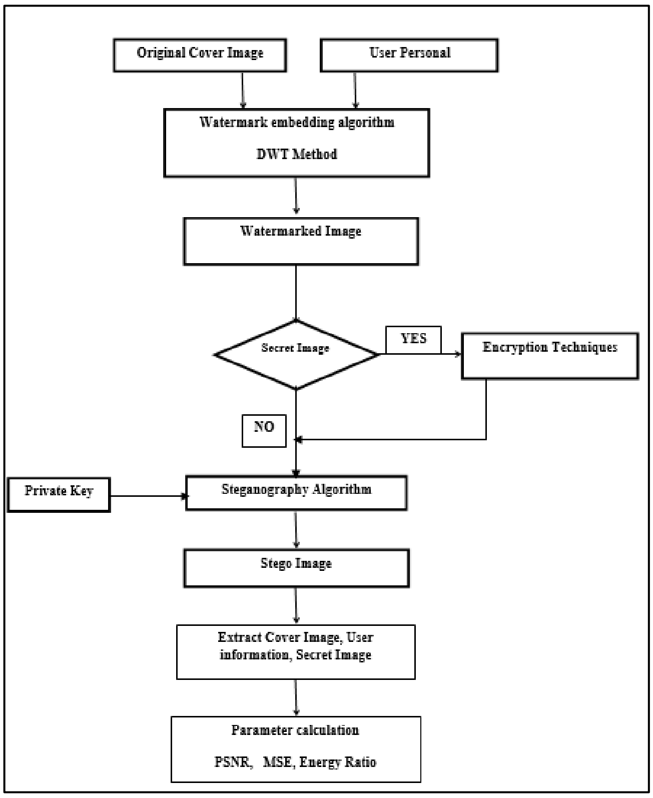


Fig. 1: Proposed Flow Chart

V. SIMULATION AND RESULT

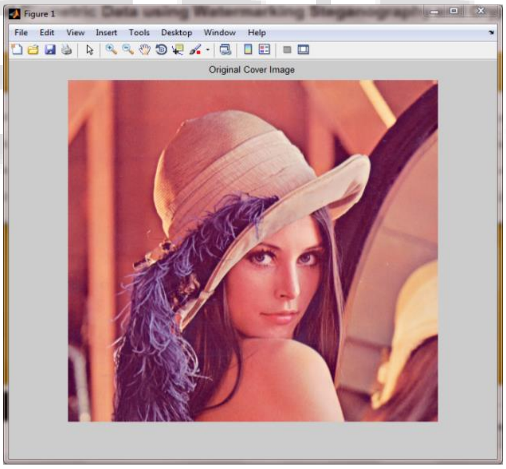


Fig. 2: Original cover image

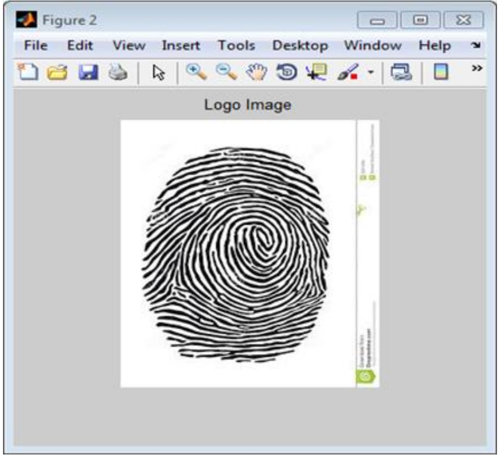


Fig. 3: User Information

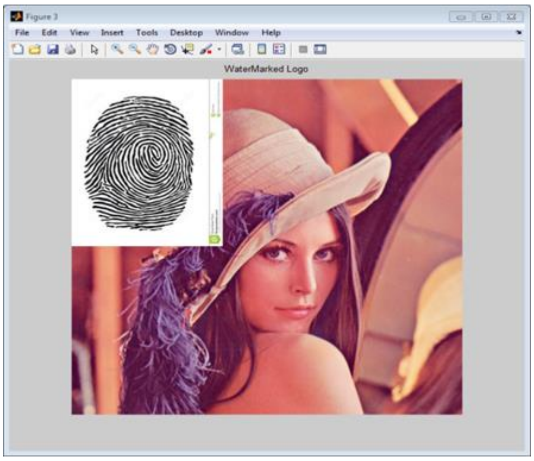


Fig. 4: Watermark Image

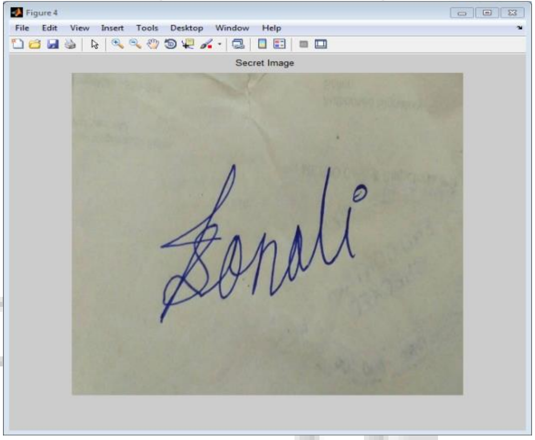


Fig. 5: Secret Image

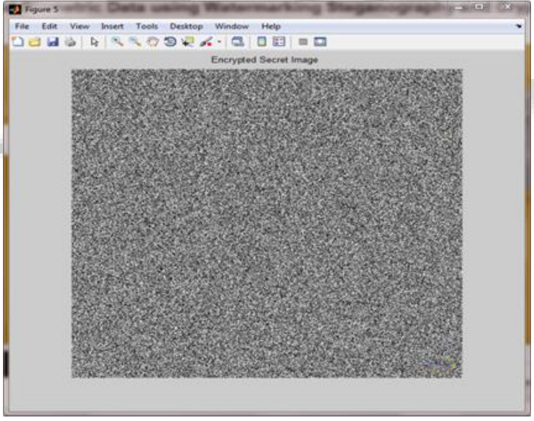


Fig. 6: Encrypted Secret Image

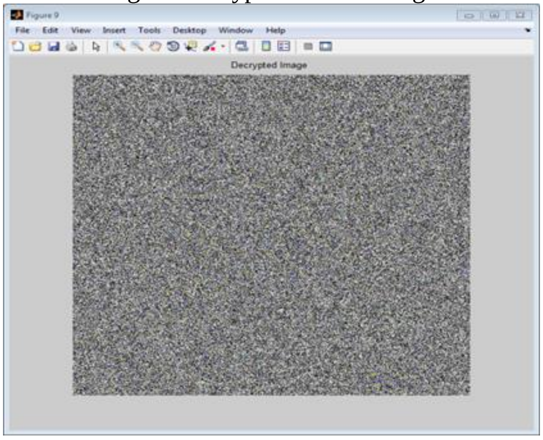


Fig. 7: Decrypted Secret Image

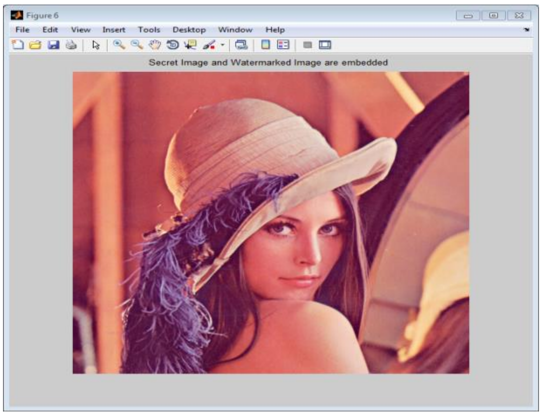


Figure 6
File Edit View Insert Tools Desktop Window Help
Secret Image and Watermarked Image are embedded

Fig. 8: Stego Image

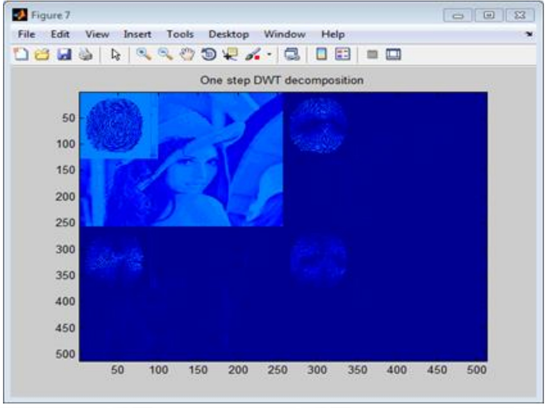


Figure 7
File Edit View Insert Tools Desktop Window Help
One step DWT decomposition
50
100
150
200
250
300
350
400
450
500
50
100
150
200
250
300
350
400
450
500

Fig. 9: DWT Output

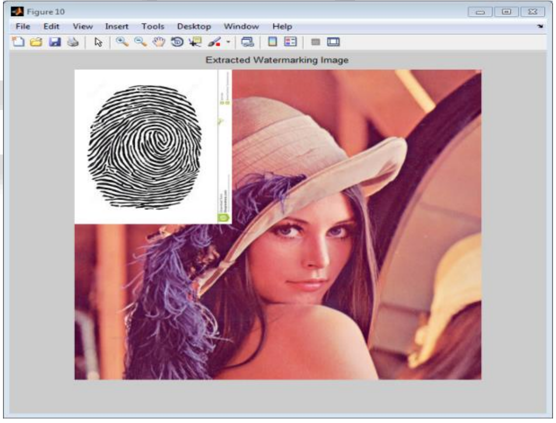


Figure 10
File Edit View Insert Tools Desktop Window Help
Extracted Watermarking Image

Fig. 10: Extracted Watermarked Image

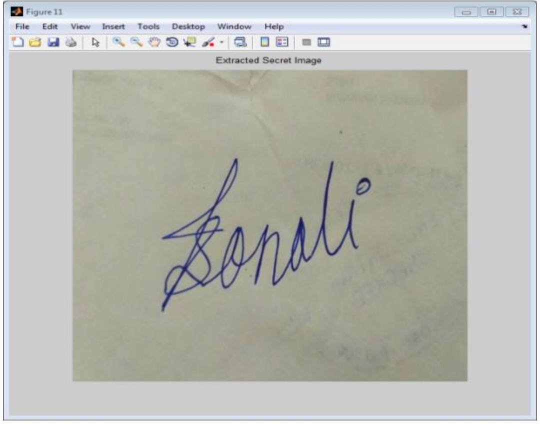


Fig. 11: Extracted Secret Image

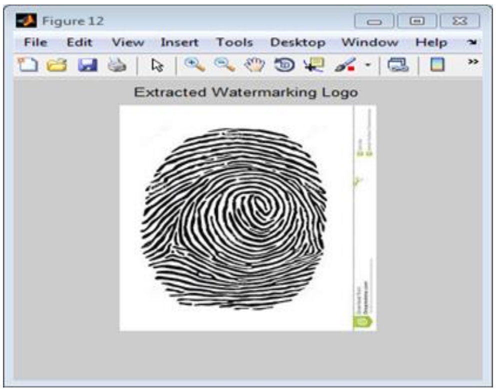


Figure 12
File Edit View Insert Tools Desktop Window Help
Extracted Watermarking Logo

Fig. 12: Extracted Watermark User Information

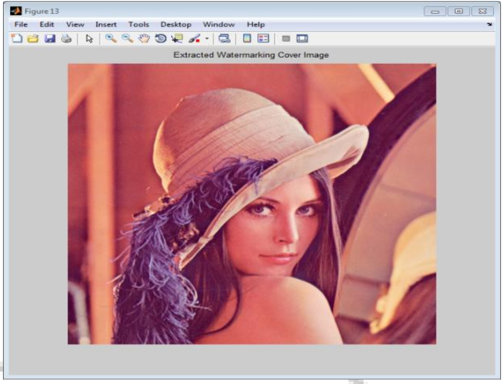
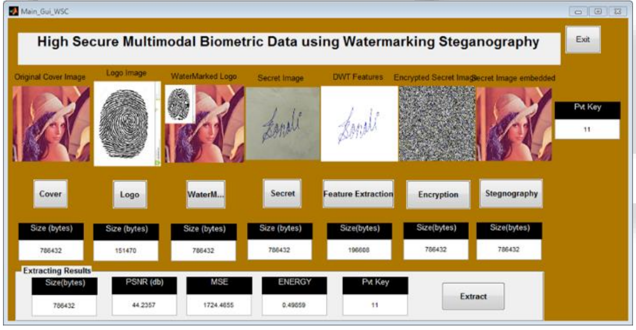


Figure 13
File Edit View Insert Tools Desktop Window Help
Extracted Watermarking Cover Image

Fig. 13: Extracted Cover Image

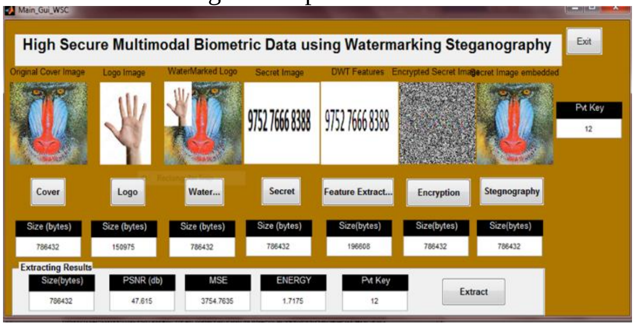


Pvt Key: 11

Size (bytes): 786432 | Size (bytes): 151470 | Size (bytes): 786432 | Size (bytes): 786432 | Size(bytes): 196608 | Size(bytes): 786432 | Size(bytes): 786432

Size(bytes): 786432 | PSNR (db): 44.2357 | MSE: 1724.4655 | ENERGY: 0.49659 | Pvt Key: 11

Fig. 14: Expected Result

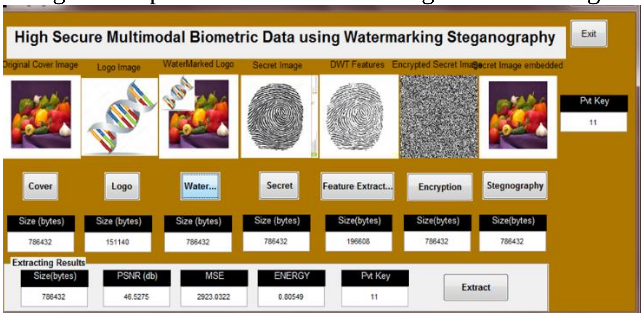


Pvt Key: 12

Size (bytes): 786432 | Size (bytes): 150975 | Size (bytes): 786432 | Size (bytes): 786432 | Size(bytes): 196608 | Size(bytes): 786432 | Size(bytes): 786432

Size(bytes): 786432 | PSNR (db): 47.615 | MSE: 3754.7635 | ENERGY: 1.7175 | Pvt Key: 12

Fig. 15: Expected Result Value Using Different Image



Pvt Key: 11

Size (bytes): 786432 | Size (bytes): 151140 | Size (bytes): 786432 | Size (bytes): 786432 | Size(bytes): 196608 | Size(bytes): 786432 | Size(bytes): 786432

Size(bytes): 786432 | PSNR (db): 46.5275 | MSE: 2923.0322 | ENERGY: 0.80549 | Pvt Key: 11

Fig. 16: Expected Result Value Using Different Image

Modified Data	Proposed work value		
	Image-1	Image-2	Image-3
PSNR	44	48	46.5
MSE	1724	3754	2923
Energy	50%	17	80
Size	786432	786432	786432
Technique Used	Watermarking, Encryption, Steganography		

Table 1: Parameter Calculation and Result

VI. CONCLUSION AND FUTURE SCOPE

Today, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit on the network. Biometrics in the high technology sector refers to a particular type of identification technologies. A motivation for the use of the techniques of watermarking and steganography in biometric systems was the need for greater security at biometric data themselves. In this paper, two simple methods steganography and watermarking are used to get a digital high security system. Both methods were applied in different images and the result was commendable. These methods can be used for the security of the image in a variety of environments. In this work, these methods are applied in any user's personal information, but these methods very well can also be used for other digital images. Yet efforts must be made to increase the capacity of inclusion and maintain digital high security system. Transform domain is the mechanism that is more secure than the pixel domain. Using steganography with cryptography it will prove to be an excellent tool in secure communication links. System security can be improved through advanced cryptography techniques and also improve efficiency through the use of data compression techniques.

REFERENCE

[1] Cameron Whitelam, Nnamdi Osia and Thirimachos Bourlai "Securing Multimodal Biometric Data through Watermarking and Steganography", IEEE 2013.

[2] Anil K. Jain, and Umut Uludag,"Hiding Biometric Data", IEEE transaction on Pattern analysis and machine intelligence,vol.25, No. 11, November 2003.

[3] Prabha jot kour "Image Processing Using Discrete Wavelet Transform", IPASJ International Journal of Electronics and Communication (IIJEC) Volume 3, Issue 1, January 2015.

[4] Mayank Vatsa, Richa Singh, P. Mitra "Digital Watermarking based Secure Multimodal Biometric System", IEEE international Conference on Systems, Man and Cybernetics 2004.

[5] Arun Kumar Singh, Juhi Singh and Dr. Harsh Vikram Singh "Steganography in Images Using LSB Technique", International Journal of Latest Trends in Engineering and Technology (IJLTET), Volume5, Issue 1, Jan 2015.

[6] Hayder Raheem Hashima, Irtifaa Abdalkadum Neamaab "Image Encryption and Decryption in a Modification of ElGamal Cryptosystem in MATLAB", International Journal of Sciences: Basic and Applied Research (IJSBAR).

[7] Shrija Somaraj and Mohammed Ali Hussain, “Securing Medical Images by Image Encryption using Key Image”, International Journal of Computer Applications (0975 – 8887) Volume 104, No.3, October 2014.

[8] Preeti Parashar and Rajeev Kumar Singh, “Digital Image Watermarking Techniques” International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124.

[9] Abbas Cheddad Joan Condell Kevin Curran Paul Mc Kevitt “Digital image steganographySurvey and analysis of current methods” Elsevierpp.727-752, 2009.

[10] Aayyushi Verma, Rajshree nolkha, Aishwarya Singh and Garima Jaiswal “Implementation of Image Steganography Using 2-Level DWT Technique” International Journal of Computer science and business information, Vol. 1, No.1,MAY 2013.

[11] Navneet Kaur and Sunny Behal “A Survey on various types of Steganography and Analysis of Hiding Techniques” IJETT, Volume 11, Number 8, MAY 2014.

[12] A.K. Jain and U. Park, “Facial marks: Soft biometric for face recognition,” in Proc. IEEE ICIP, 2009, pp. 1–4.

[13] Hongrui Wang, Jianli Yang, Haijun Sun, Dong Chen, Xiuling Liu, “An improved Region Growing Method for Medical Image Selection and Evaluation Based on Canny Edge Detection”,2011 IEEE.

[14] Ramadhan, J. Mstafa, Khaled, M. Elleithy and Eman Abdelfattah “A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC” IEEE, vol. 5, April 2017.

[15] Mayank Garg, Shashikant Gupta and Pallavi khatri “Fringerprint watermarking and steganography for ATM transaction using LSB-RSA and 3- DWT Algorithm” IEEE, International Conference on Communication Network 2015.

[16] Palak Patel and Yash patel “Secure and Authentic DCT Image Steganography through DWT-SVD Based Digital Watermarking with RSA Encryption” IEEE, International Conference on Communication System and Network Technologies, OCT.2015.