Defending Biometric Templates by Multilevel Authentication using BioCryptography and Steganography Techniques

T. Leena Premakumari[#1], Dr. S. Arul Jothi[*2]

[#]Assistant Professor, Dept. Of Information Technology, Fatima College, Tamilnadu, India

*Assistant Professor, Dept. Of Computer Science, Fatima College, Tamilnadu, India

Abstract *Defending information against some intruders is a most demanding task in our computer world. Now a day's information sharing and transferring are the common task performed over the network. In this paper we are defending the biometric templates from the malicious users. Biometric templates may be modified by attacker. Here we are using steganography techniques and biocryptography techniques as a multilevel authentication. Biometric is a method of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics such as knuckles, skin, nail etc. The biometric system offers a greater security when compared to the password authentication or token based system. Biometric templates are acquired from the subject as a raw biometric data and we are extracting a feature from the data and compare the feature set against the template stored in the database in order to identify the person. And at the same time it is possible for the intruders to identify or access the data from the database where the data is stored as the biometric data. So defending the data is the major concern for that we are using the following techniques such as steganography and biocryptography. In biocryptography we can defend the important data from the hackers. Cryptography provides the means to further protect Biometric Templates at these critical junctures. It is the science of scrambling information and data which is transit across a network medium, and then descrambling it at the receiving end into a decipherable format. That way, if the scrambled information and data were to be intercepted by a third party, there is not much which can be done unless they possess the keys for descrambling the information. These concepts of scrambling and descrambling can be very easily applied to biometrics. This is known as "Bio-Cryptography". The next level of protection is by using the steganography which is one of the major techniques used for secret communication. "Steganography is an art of sending secret messages over public channel in such a way that only the intended recipient knows about the existence of the message" and it is a skill as science of hiding a top secret communication in a cover media such as image, text, signal or sound in such manner that nobody, apart from the deliberate recipient knows the existence of the data In other words, the biometric templates are protected by scrambling and descrambling keys while they are stored in the database, or in movement across a network.*

Keywords — *Steganography, Biocryptography, biometric templates, keys, Intruders, hackers.*

I. Introduction

Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words "bio" meaning life and "metric" meaning to measure. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include skin, knuckles, iris, nail, DNA and signatures. The oldest form of biometric verification is finger prints. Historians have found examples of thumbprints being used as a means of unique identification on clay seals in ancient china. Biometric verification has advanced considerably with the advent of computerized database and the digitization of analog data, allowing for almost instantaneous personal identification. Biometric templates also called templates is a digital reference of distinct characteristic that have been extracted from a biometric sample. Templates are used during the biometric authentication. It is a snapshot of our physical behavioral is what is being captured or analyzed. This could be an image ranging from the shape of our hand to our finger, or our eye or even when we speak. This image can be a master profile then from this that the unique feature can be extracted and then converted into a mathematical file. This file can be anything from a binary mathematical file to a statistical model. It is these mathematical files which become known as the biometric templates not the images which were extracted and created. What happen when the biometric templates get stolen or hacked? For example: What can hacker do with a series of zeroes and ones and/ or a probability curve? It is not the same as stealing the credit card number. A biometric vendor has the his own proprietary, mathematical enrollment and matching such as verification and identification algorithms so taking a template and putting into another system is simply not feasible. But , if one were to dig deeper at the technical level Biometric templates are just like any other technology, which are prone to failures, hacking and at granular could to a certain degree be reversed engineered.

There are four critical areas where Biometric Templates are at most risk to hacking and theft, and they are as follows:

- Just after template creation (this includes both the verification and the enrollment templates).
- The biometric templates which are housed in the database (the actual database depends upon the specific biometric technology being used).
- In client server network topology, the transmission of biometric templates from the biometric system to the central server (this is where the biometric database resides);
- In a hosted environment , there the biometric template database resides with a third party

Cryptography provides the means to further protect biometric templates at these critical junctures. It is the science of scrambling information and data which is transit across a network medium, and then descrambling it at the receiving end into a decipherable format. That way, if the scrambled information and data were to be intercepted by a third party, there is not much which can be done unless they possess the keys for descrambling the information. These concepts of scrambling and descrambling can be very easily applied to Biometrics. This is known as “Bio-Cryptography”. In other words, the biometric templates are protected by scrambling and descrambling keys while they are stored in the database or in movement across a network. Proper use of cryptography greatly reduces the risks in biometric systems as the hackers have to find both secret key and template. It is notified that still fraud rant goes on to some extent. Here in this paper a new idea is presented to make system more secure by use of steganography with the help of the secret key that we get from the bio cryptography (which is in the form of pixel intensities) will be merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode.

II. Cryptography and its Progression

In early stage the cryptography was used to convert the message in to an unreadable form to individual users or group to prevent the message content during the transfer. In recent era cryptography has grown from the basic level of confidentiality by including integrity, checking, sender and receiver identity authentication and digital signature. The earliest form of cryptography was encompassed by Egypt, Greece and Rome.

In 1900BC Egyptian used hieroglyphs a non standard fashion presumably to hide the meaning from those who didn’t know the meaning. The Greek’s idea was to wrap a tape around a stick and then write the message on the wound tape. But, when the tape was unwounded the writing would be meaningless. In the receiver side they have a stick of the same diameter and used it to decipher the message. The method of cryptography was known as Caesar Shift Cipher. In this method the letters are shifted by an agreed number and thus writing the message using the letter shifts. In the destination side they shift the letter back by the same number and decipher the message as in [1].

The Caesar Shift cipher is an example of Mono alphabetic Cipher, but in this method the hackers can easily break the code. This method is breakable by using the frequently analysis attributed to Arabic Circe 1000 C.E. In this method the frequently used letters are identify and easily the intruders can try to substitute known frequently used letters.

The progression of the Cryptography doesn’t show any changes or advancements until the middle ages. The Western European governments were utilizing cryptography in one form to another. Leon Batista Albert was known as the Father of Cryptology. He used the Poly alphabetic Substitution. In this method two copper disks that fit together each one of them had the alphabet inscribed on it, after every few words the disks were rotated to change the encryption logic. So the frequency analysis is limiting to crack the cipher as in [2]. This poly alphabetic substitution went through the variety of changes and beyond this the most notable is vigenere by Rubin.

Gilbert Vernam went through the work and improved the broken cipher creating the Vernam_Vignere cipher in 1918. But, he can’t create it with greater strength. Next Whiteman reports that the criminals used the Cryptography during the prohibition to communicate with each other. Later in 2005 Navojo’s used ‘Windtalker’. In modern times the common Public key and private keys held only by the sender is the asymmetric encryption as in [3,4]. The sender uses the private key to encrypt the message and in the destination the receiver use the public key to decipher the message. So now a day’s Encryption and decryption techniques are followed with the different kind’s algorithms. The Encryption is of two types.

A. *Encryption Methods*

i) One way Encryption:

It is a mathematical function that takes a variable length input string and converts it into a fixed length binary sequence. It is hard to reverse the process

ii) Two Way Encryption:

This encryption method is used when the encrypted information needs to be restored back to the original information.

III. STEGANOGRAPHY AND ITS IMPORTANCE

Steganography or stego literally means the 'covered writing' which is derived from the Greek language. It is an art and science of hide the message inside other harmless message, graphics and sound. The techniques comes from the Greek stegnos (Covered or secret) and graphy (writing or drawing).The technique have been used by the ancient Greek in 440BC.The goal is to communicate the message the modern application is also same but to hide the message as a secret data in a cover and send to the proper recipient who knows to decipher the hide message as in [5]. The communication can't be detected by the third parties.

Herodotus tells how a message was passed to the Greeks about Xerses intimidating intention beneath the wax of a writing tablets and letters in a cover text with a secret link due to Aeneas the Tatician. Historical methods depends on Physical stenography such as pirate legends tells, that tattooing a secret information such as a map on the head of someone so that the hair would conceal it or in the human skin , games etching advance the hiding is based in the use of more complex covers example with aid of ordinary objects. The world war had accelerated the development of steganography by introducing a new carrier the electromagnetic waves. There are various tricks to be followed to hide the message.

The first one is war telecommunication which use spread spectrum or meteor scatter radio in order to conceal both the message and it source. In Industrial market with the advent of digital communication and storage, one of the most important issues is copyright enforcement. Digital watermarking techniques are being developed to restrict the use of copyright data as in [6]. Next is embedded data about medical images, so that there is no problem with matching patient records and images.

Hidden message were hard to interrupt within the innocent message for example "Fishing freshwater bends and saltwater coasts reward anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day. "

By taking the third letter in each word the following message emerges: Send Lawyers, Guns, and Money.

Steganography in the digital age used the images and sound carriers files called Least Significant Bits Substitution or overwriting. For example

10010101000011011100100110010110

00001111110010111001111100010000

Underlined are the Least Significant Bits in each byte group. The significance of these bits is so minor when compared to the whole, that altering these bits could produce close to the same result.

10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001

Only half of the Least Significant Bits were changed in the virgin sample, and yet the character G has been discretely imbedded into the sequence. Judging from the amount of bits needed to make even the simplest of files, it is easy to imagine just how much hidden data can be secretly embedded using Least Significant Bit Substitution.

The future of steganography is the digital water marketing which navigate to the future of security. It is a kind of marker covertly embedded in a noise tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal.

In this paper the biometric templates which are encrypted by the cryptography technique and the keys that used are covered by the digital water marking by the steganography technique.

IV. ENCRYPTING BIOMETRIC TEMPLATES USING BLOWFISH ALGORITHM:

Cryptography is a widely used technique it is a study of methods of sending message indistinct form so that only the intended recipient can remove the disguised message and read the message. They encrypt the plain text to generate cipher (encrypted) text. Data that can be read and understood without any special measures is called plaintext or clear text. This method is called encryption. The process of converting plain text to a cipher text and disguised message is called enciphering or encryption, and the reverse process is called deciphering or decryption. Cryptology and cryptanalysis are two main branches of cryptography. Cryptology is to keep plaintext secret from eavesdropper or simply the enemy while cryptanalysis deals with the defeating such techniques to recover information. In this paper the Biometric templates such as skin spectroscopy, nail plates and knuckles are encrypted using the blowfish algorithm to get an encrypted biometric template. There are various Cryptographic algorithms used for encryption of the data in this paper we use the blowfish which has lot of advantages when compare to the other cryptographic algorithms. The advantages of blowfish are 1) Block cipher of 64 bit which can also be used as a replacement for the DES algorithm. 2) It takes a variable length key ranging from 32 bits to 448 bits default 128 bits. 3) It is fast as its encryption rate on 32 bit microprocessor is 26 clock cycles per byte. 4) It is compact as it can execute in less than 5kb memory 5) It is simple because it uses only primitive operations like addition, XOR and table lookup, making its design and implementation simple. 6) It has a variable key length up to a maximum of 448 bit long making it both flexible and secure .7) No attack is known to be successful against this. 8) It is unpatented, license free and is available free for all uses. The bio templates such as skin, knuckles and nail plates are taken as a data and encrypt the data using the key generated by the blowfish algorithm as in [7].

B. Algorithm Explanation:

There are two pars to this algorithm i) to handle the expansion of the key and ii) to handle the encryption of data.

1) Key Expansion:

- To break the original key into a set of sub keys. [A key of number more than 448 bits is separated into 4168 bytes.]
- There is a P- array and four 32 bit S-boxes.
- The P-array contains 18, 32- bit sub keys while each S-boxes contains 256 entries

2) Encryption:

The following steps are used to calculate the sub keys:

- Initialize the biometric templates.
- Use the keys such as XOR P-array with the key bits
- Use the above method to encrypt the all the Zero string
- The new output is P1 and P2.
- Encrypt the new P1 and P2 with modified sub keys.
- This new output is considered as P3 and P4
- Repeat 521 times in order to calculate new sub keys for the P-array and the four S- boxes
- Finally we get the encrypted Biometric template.

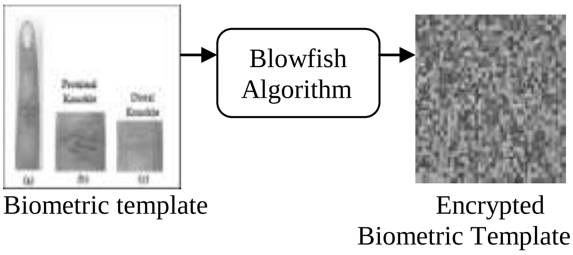

Fig. 1 Encryption

V. HIDING THE ENCRYPTED BIOMETRIC TEMPLATE USING DIGITAL WATERMARKING:

In Steganography it hides the secret message in the plain sight rather than encrypting the message it embedded the data and doesn't require any secret transmission. The message received by the recipient is carried inside the Image or sound or in any other format. It can be used in a large amount of data format ssuch as .bmp, .doc, .gif, .jpeg, .txt and .wav. These technologies are very important part in the future of Internet security and privacy. The use of steganography arrives because of the weakness in the cryptographic system when it is used in the open system environment. And many of the government laws that limit the strength of cryptosystems or prohibit them completely as in [8]. This leads to a weak and easily breakable encryption algorithm. Steganography is used to hide the data inside another file so that the recipient intended to get the message only knows the secret message.

Neither the Steganography nor Cryptography is considered as a best solution for open system privacy. But using the both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these Systems. In this paper we use the Digital watermarking to hide the Encrypted biometric templates. Digital watermarking is the process of adding identifying data, to digital content such as text, image, film, music and software programs. There are two types of digital watermarking that ate perceptible to the human eye or ear. Both are used without affect the quality of the content during compression and decompression, encryption and decryption as in [9]. It is used to identify the originator or authorized user and verify the authenticity or integrity of the data.

VI. FRAMEWORK FOR WATERMARKING:

It is used to hidden the message within a digitized image, video or audio recording. It requires no additional storage space.

Watermarking Schemes consists of three parts.

1. The watermark
2. The encoder (insertion algorithm)
3. The decoder (extraction or detection algorithm)

We can have a unique watermark or different watermarks in different objects. The marking algorithm incorporates the watermark into the object as in [10]. The verification algorithm authenticates the objects determining both the owner and the integrity of the object.

`1) ***Encoding Process:***

Let I denotes Image and a signature by S=s1,s2…sn. E is the encoder function it takes an image I and a signature S and it generates a new image which is called Watermarked Image I.

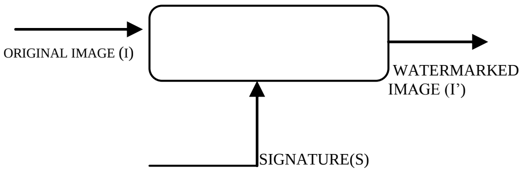

Fig. 2 Encoding Using Watermarking

*2) **Decoding Process:***

A decoder function D takes an image K (K can be a water marked or UN watermarked image and possibly completed) it determines and recovers a signature S' from the image. In this process an additional image I can also be included which is often the original and unwatermarked version of K.

D =(K, I)=S'

The extracted signature S' will then be compared with the original signature sequence by a comparison function and a binary output decision generated as in [11]. It is 1 if there is a match and 0 otherwise.

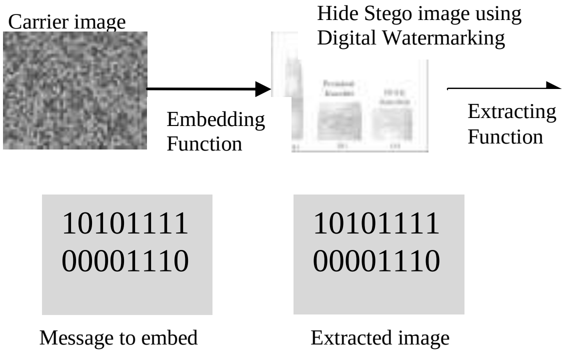

Fig. 2 Decoding Using Watermarking

VII. Conclusion

In this paper the biometric templates are prevented from the hackers or illegal users for authentication purpose here we use multilevel authentication techniques such as cryptographic and steganography. The biometric templates are encrypted with the help of blowfish algorithm which is one of the best algorithms when compared with the other encryption algorithm and then encrypted biometric templates are hiden using the steganography technique such as digital watermarking which can't be easily detected by the unauthorized persons. So the cryptographic or steganographic technique which can be used alone is not an effective one for authentication purpose but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

References

[1] K. S. Sandha, "Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology, vol. 2, Sep. 2011.

[2] D. Das, J. Nath, M. Mukherjee, N. Chaudhury and A. Nath, "An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE conference WICT-2011 held at Mumbai University, Dec. 2011.

[3] J. Nath. et. al. "Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method: TTSJA algorithm", IJCA, Vol. 42, Mar. 2012.

[4] D. Chatterjee, J. Nath, S. Das, S. Agarwal and A. Nath, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at Las Vegas, USA, July 2011.

[5] Ismail Avcıbas, Nasir Memon, and Bülent Sankur, "Steganalysis Using Image Quality Metrics", IEEE Transactions On Image Processing, vol. 12, Feb. 2003.

[6] Ajay.B.Gadicha, "Audio Wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), vol. 1, Nov. 2011.

[7] Pratap Chnadra Mandal, "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering , vol. 2, Sep. 2012.

[8] J. Daemen and V. Rijmen, "Rijndael: The Advanced Encryption Standard", Dr. Dobb's Journal, Mar. 2001.

[9] M. Sreerama Murty, D. Veeraiah, and A. Srinivas Rao, "Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis," Signal & Image Processing : An International Journal, vol. 2, pp. 170–179, Jun. 2011.

[10] J.S. LeenaJasmine, L. Prabha, "An Efficient Secure Image Watermarking Using Wavelet Transform", International Journal of Computer Trends and Technology, vol. 17, pp. 133–137, Nov. 2014.

[11] G.Shyamala, I.Jasmine Selvakumari Jeya and M.Revathi, "Secure and Reliable Watermarking in Relational Databases", International Journal of Computer Trends and Technology, vol. 11, pp. 13–18, May. 2014.