The Role of Security Techniques in Biometric System

Jyotika Chopra

ECE Department & RIMT-MAEC, Mandi Gobindgarh

jyotika.chopra1@gmail.com

***Abstract*— A biometric system essentially is a pattern recognition system that makes a personal identification on the basis of a specific physiological or behavioral characteristic possessed by the user. As biometric system provides us many advantages over traditional methods but still there are pros and cons of every developed system. There is main issue involved if the biometric key we are using if it will be stolen, then what will happen? So the system needs security , in this paper security techniques are discussed , from it is concluded that the watermarking technique will improve the system performance.**

***Keywords*— Watermarking, Biometric System, key, Security**

I. INTRODUCTION

Biometrics based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards (ID), passwords, token etc. One of the main reasons for this popularity is the ability of the biometric technology to differentiate between an authorized person and a fraud person who acquires the access privilege of an authorized person [1]. Among various available biometric techniques such as face, voice, fingerprint, iris, etc., fingerprint-based techniques are the most extensively used as the advantage of using this biometric system is that the information is unique for each individual and that it can identify the individual in spite of variations in the time (it does not matter if the first biometric sample was taken a year ago). With the rapid development of network distributions of digital media contents, there is an urgent need for copyright protection against plagiarism. There is a solution to copyright protection problems, many digital watermarking schemes have been proposed for intellectual property right protection of digital media data. [4]

II. BIOMETRIC SYSTEM

A biometric system essentially is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic. A biometric system can be either an identification system or a verification (authentication) system; both are defined below:

A. Identification

A comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

B. Verification

A comparison of two sets of biometrics to determine if they are from the same individual. It can be done in conjunction with a smart card, username or ID number. During registration, template samples are captured by either fingerprint scanner or video camera. Biometric systems can identify or verify a person by fingerprint, face, iris, retina, voice, signature etc. To authenticate the specified person, all biometric systems involve following steps: capture, extraction, comparison, and match/non match.

III. NEED OF SECURITY

In a world full of security threats we are facing internal and external problems. According to this scenario, most people are really worried because of their safety. Numerous organizations choose different equipment to make sure the safety of the site, however you can find still many of the body, and that is the manual system to continuously monitor visitors, customers and also employees. [7] As this kind of traditional systems of a number of disadvantages, like the not enough accuracy, the most time-consuming and does not provide the total loss of safety. Now a day's many organizations require using biometric security solutions, such as different types of fingerprint readers, show-card devices, face acknowledgement system and many more.

IV. APPLICATIONS OF BIOMETRIC SYSTEM

The Biometric system has become a crucial part of our life. It has given us very advantages of using these technologies. The few usage of this technology is listed below:

A. Home Security Advances – Biometric Locks

Biometric Lock Technology is introduced in our daily life to provide protection to our home system. Moreover, if we choose a biometric entry, we will never have to worry about losing keys, as it might be the case with a traditional key lock. Besides, there is no need to be worried about forgetting pins which usually happens with keypad locks. All we need to do is just to scan our finger, and we will easily get into your home.

B. Chase Militant

Biometrics refers to the identification of a people on the basis of their physical and behavioral characteristics. Today we know various biometric systems that are based on the identification of these, for everyone's unique identity. Some biometric systems include the characteristics of: fingerprints, hand geometry, voice, iris, etc., and can be used for identification. [6] Most of the biometric systems are based on the collection and comparison of biometric characteristics which can provide identification. Biometrics methods are used to chase the militants in the U.S. In the prison, eye scans, fingerprints and facial images of each militant are recorded and for future purpose it plays a very effective role.

C. . Gas Station Robbery

In2000, Hoogstrate et al. (2000) from The Netherlands' Forensic Institute describe a small experiment, where ear pictures and ear identification are used to find out gas station robbery. Through 38 years of research and application in earology, the author has found that in literally thousands of ears that were examined by visual means, photographs, ear prints, and latent ear print impressions, no two ears were found to be identical not even the ears of any one individual. However in the Netherlands the court decided that the earmarks are not reliable enough for judging (Forensic-Evidence News, 2000).

V. VICISSITUDE OF BIOMETRIC SYSTEM

As we know that biometrics are the oldest forms of identification. Humans recognize faces. On the telephone, your voice can be authenticated. Your signature identifies you as the person who signed a contract. In order to be useful, biometrics must be stored in a database. As we take example, Jam's voice biometric system works only if we recognize his voice; it won't help if he is a stranger. We can verify a signature only if we recognize it. To figure out this difficulty, banks keep signature cards. Jam's signs his name on a card when he opens the account, and the bank can verify Jam's signature against the stored signature to ensure that the check was signed by Jam.

There is a variety of different biometrics. In addition to the three mentioned above, there are various other biometric systems as hand geometry, fingerprints, iris scans, DNA, typing patterns, signature geometry etc. The technologies are different, some are more reliable, and they will all improve with time. Biometrics is hard to design and it is hard to put a false fingerprint on your finger, or make your iris look like someone else's. Some people can mimic others' voices, & Hollywood can make people's faces look like someone else, but these are specified or expensive skills. When we see someone sign his name, we generally know it is he and not someone else.

If the verification takes place all over the network, the system may be unsecure. A hacker won't try to forge Jam's real thumb, but will instead try to inject his digital thumbprint into the communications. Biometrics also can't manage failure well. As we can take example of Jam is using his thumbprint as a biometric, and someone steals the digital file. Now what next? This isn't a digital certificate, where some trusted third party can issue his one. Once someone steals our biometric, it remains stolen for life there is no getting back to a secure situation. And biometrics is inescapably common across different functions. Just as we should never use the same password on two different systems, the same coding key should not be used for two different applications. If the fingerprint image is used to start my car, unlock my medical records, and read my e- mail, then it is not hard to imagine some very unsecure situations arising.

Biometrics is powerful and useful, but they are not keys. They are not useful when you need the characteristics of a key: secrecy, the ability to update or destroy. They are useful as a replacement for a PIN, or a replacement for a signature. They can sometimes be used as passwords that a user can't choose a weak biometric in the same way they choose a weak password. Biometrics is useful in situations where the connection from both end is secure.

VI. VARIOUS SECURITY TECHNIQUES

Due to the illegal usage of biometric systems, need of security of the biometric system arises. There are various ways by which we can secure our biometric system that are stenography, watermarking and cryptography. With the breakneck breakthrough of network technology, multimedia information is transmitted over the Internet easily. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. Security issues should be taken into consideration while communicating the secret images, because hackers may utilize weak link over a communication network to rob information that they want. to deal with the security problems, various image cryptographic schemes have been developed to share and communicate the secret

image. Visual cryptography was introduced by Naor and Shamir in 1994 to protect the secret images. Unlike other cryptographic technique, decryption can perform by the human visual system without the aid of a computer system. But watermarking is best technique.

VII. WATERMARKING SYSTEMS

A watermarking scheme consists of three parts: the watermark, the encoder, and the decoder and comparator [Memon and Wong 1998]. The watermarking algorithm fused the watermark into the object, whereas the verification algorithm authenticates the object by determining the presence of the watermark and its actual data bits. Available techniques use different transform domains to embed the watermark inspired by information coding and image compression. The watermarking is performed in the cover image through several domains such as discrete cosine transform (DCT), discrete wavelet transforms (DWT) and discrete Fourier transform (DFT) [Mohanty et al. 2006]. Digital watermarking can be defined as the process of embedding by means of a secret key .Based on human perception, digital watermarks can be either visible or invisible. A visible watermark is a secondary translucent mark covered in the primary image. This has been used since very long time which is not secure watermarking. This type of Watermarking could use only for owner identification process .The invisible watermark is embedded in such a way that modifications made to the pixel value are perceptually unnoticeable and can be recovered only with an appropriate decoding mechanism. In this watermarking the embedded data is not detectable, but may be extracted or detected by a computer program.

Embedding multiple watermarks is proposed to embedding a single watermark, and which is used to detect a randomly selected subset of them while constraining the embedding distortion. [1] The configuration of the scheme lies in both watermark generation, which distributes a family of one-way functions and selective detection, which injects uncertainty into the detection process. The potential of this approach in reducing the false-positive probability is analyzed under various operating conditions and compared to single watermark embedding. And the results obtained under a numerous conditions which shows that the false-positive probability can be indeed decreased with the use of the scheme, and it is robust under additive white noise attacks. [Husrev et al. 2007]

Proxy-Based Partitioning scheme is used on mobile for the watermarking. In a digital file which contains audio, image, text, or video data. The watermark can be used to authenticate the data file and for tamper detection. It is particularly valuable in the use and exchange of digital media, such as audio and video, on emerging handheld devices. Digital watermarking has been proposed as a technique for securing an intellectual property of digital data. It is the process of coding a signature/watermark into a digital media file so that it is hidden from view, but can be extracted on demand to verify the authenticity of the media file. [2] The watermark can be a binary data, a logo, or a seed value to a pseudorandom number generator to produce a sequence of numbers with a certain distribution. It is based upon ongoing advances in digital watermarking and proxy-based middleware services. The use of proxies as agents that can connect to a range of heterogeneous clients is a well- accomplished practice. [Arun et al. 2006]

A potential application scenario for visible watermarks was proposed by IBM where an image is originally embedded with a visible watermark before posting on the web for free observation and download. The watermark can be removed to recreate the unmarked image by request of interested buyers. Before we can develop an algorithm for satisfying this application, three basic problems should be solved. First, we need to find a strategy suitable for producing large amount of visually same but numerically different watermarked versions of the image for different users. Second one is that the algorithm should let the embedding parameters reachable for any legal user. Third, an unauthorized user should be prevented from removing the embedded watermark pattern. In this a user-key-dependent removable visible watermarking system. The user key structure decides both the embedded element of watermark and the host information adopted for adaptive embedding. The neighbor-dependent embedder adjusts the marking strength to host features and makes unauthorized removal very difficult. With correct user keys, watermark removal can be accomplished in "informed detection" and the high quality unmarked image can be restored. In contrast, unauthorized operation either overly or insufficiently removes the watermark due to the wrong estimation of embedding parameters, and thus, the resulting image has apparent defect.

A robust watermarking algorithm using balanced multiwavelet transform is proposed. The embedding scheme using a modified version of a well-established perceptual model. Therefore, the strength of the embedded watermark is controlled according to the local properties of the image. This has been achieved by the proposed perceptual model. This adaptivity is a key factor for achieving the imperceptibility need often used in watermarking applications. In addition, the watermark embedding scheme is based on the principles of spread-spectrum communications to achieve higher watermark robustness. The optimal bounds for the embedding capacity are derived using a statistical model for balanced multiwavelet coefficients of the host image. Finally, the analytical expressions are contrasted with experimental results where the robustness of the proposed watermarking system is evaluated against

standard watermarking attacks. [4]

In many image processing scenarios, it would be desirable to embed a watermark on an image right after acquisition in order to ensure that no unwatermarked version of the original image is stored or distributed. In such cases, the image might later undergo image processing operations before distribution. In other cases, an attacker might perform image scaling as part of his malicious attack [5]. In the very common case of image resizing at dimensions larger than the original, the watermark information, which was embedded in the low-resolution version upon acquisition, is spread on the larger image. The larger image could then be compressed and transmitted to any potential recipients (in a lawful distribution scenario) or distorted in the case of a malicious attack. [Alexia Giannoula et al.2006].

Watermarking is one of several techniques available today to deter copyright infringement in electronic systems. The technique consists of implanting stamps in the circuit's inner structure, while not disrupting its functionality nor degrading its performance significantly. In this paper, a novel method is proposed for the creation of watermarks in regular sequential functions. [6] This is an important class of functions, as it is the basis of most digital controllers. Algorithms are proposed for implanting robust watermarks to minimize the overhead and, ultimately, to reduce the impact on performance. Detection methods have been discussed in the presence of infringement attacks. [Ilhami Torunoglu et al.2000]

Digital watermarking technology is emerging as a solution to a broad class of information communication challenges such as self-healing data, broadcast monitoring, and signal tagging. In these applications, compression is the most common form of incidental distortion to limit the robustness of watermarking. Correlation expressions between the embedded watermark and the extracted watermark are used to determine the optimal watermarking domain to maximize data hiding rates for spread spectrum and quantization watermarking. when the quality [7] level is less than 75, the hybrid algorithm tracks the spread spectrum method as the latter has superior performance. [Chuhong Fei et al. 2004]

Biometric fingerprint watermark message in digital format will be embedded into a copyright material image by Discrete Cosine Transform (DCT) for copyright ownership authentication. During the embedding process, copyright material image and the fingerprint watermark message will be adaptively partitioned and then DCT method will be applied to each partition for embedding and extracting the watermark message. Traditionally, they may deposit copies of their work with a bank or solicitor; or send copies to themselves by special delivery which gives a clear date stamp on the envelope, leaving the envelope unopened when it is returned to them. Either of these methods could help to prove that their work existed at a certain time. But nowadays, globalization and use of internet make these traditional methods impractical. An electronic copy can be easily obtained by just a simple click and its creation time stamp can be adjusted by some sorts of applications. [10]. Facing these technical challenges, how can we protect our copyright materials from being unauthorized even distributed? Adopt an instant download permission key to open a copied multimedia file and on-line database? Embed a visible security overlay in a duplicated electronic artistic works? But these methods can merely increase the difficulties on the access to the material. In respect to the ownership authentication of a copyright material, hiding some invisible personalized information as an authentication key can be a considerable method.

An adapting digital watermark algorithm based on the image fusion and chaos is put forward [Zhang Fan et al .2009] The chaos phenomenon comes up in the misalignment dynamic system and has sensitive dependence on initial situation, similar noise, non-cycle, definite, and similar random process. The image fusion carries a synthesis processing on many images that from different sensors, thus obtains a new image that can meet some kind of requirements.

An efficient watermarking technique for use to protect fingerprint images. The rationale is to embed the watermarks into the ridges area of the fingerprint images so that the technique is inherently robust, yields imperceptible watermarks, and resists well against cropping and/or segmentation attacks. The key features of the proposed technique are to (i) preserve the watermark from segmentation which can be considered as a special case of the cropping attack, (ii) increase the robustness of the watermark against known attacks such as filtering, noise, and compression, and (iii) allow to embed imperceptible watermarks by embedding in highly textured areas.

Watermarking methods are often evaluated based on the common properties of robustness, tamper resistance, and fidelity. However, examination of these properties without careful consideration of the application can often be misleading. A watermark designed to serve security needs of the CIA must meet different requirements than one intended for annotating home video. Thus, it is inappropriate to evaluate these two watermarks according to the same standards. The applications of watermarking are broadcast monitoring, owner identification, proof of ownership, authentication, transactional watermarks, copy control and covert communication. Watermarking is a technology that can serve a wide variety of applications, each of which may have very different requirements. Each application dictates a different tradeoff between the properties of robustness, tamper resistance, fidelity, and false positive rate.

VIII. CONCLUSION

As the Biometric system has many advantages over traditional methods as their no need to remember the passwords, only physiological or behavioral characteristic of the specified plays great role. Due this usage, biometric system plays a vital role in our life .Various examples are discussed in which importance of few biometric system are discussed. But still it need improvement in point of view of security. If the biometric key that we are using, if it will be stolen by third unknown parties. Then what will be next steps? So this problem will be minimized to some extent with the help of several security techniques. Best technique which will improve the performance of the biometric system is the watermarking. Few literature surveys are discussed on the basis of watermarking technique which also ensures that the hiding of data on the basis of some coding or key it is possible only with the biometric technique.

REFERENCES

[1] Husrev Taha Sencar and Nasir Memon, "Combatting Ambiguity Attacks via Selective Detection of Embedded Watermarks"IEEE Transactions on Information Forensics and Secuirty, Vol. 2, No.4, pp 664-682, December 2007.

[2] Arun Kejariwal, Ed., " Energy Eficient Watermarking on Mobile Devices using Proxy- Based Partitioning," IEEE Transactions on Very Large Scale Integration Systems, vol.14,No.6 pp 625-66 June 2006

[3] Yongjian Hu, Sam Kwong, and Jiwu Huang," An Algorithm for Removable Visible Watermarking," IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, No. 1, pp129-133, January,. 2006.

[4] Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, "Digital Image Watermarking "Using Balanced Multiwavelets," IEEE Transactions On Signal Processing, Vol. 54, No. 4, pp 1519-1536, April 2008

[5] Alexia Giannoula, Nikolaos V. Boulgouris, Dimitrios Hatzinakos, and Konstantinos N. Plataniotis, "Watermark Detection for Noisy Interpolated Images" IEEE Transactions On Circuits And Systems—II: Express Briefs, vol.53, No. 5,Pp 359-363 May 2006

[6] Ilhami Torunoglu and Edoardo Charbon ," Watermarking-Based Copyright Protection of Sequential Functions", IEEE Journal of Solid-State Circuits, vol. 35, No. 3,Pp 434-440,February 2000.

[7] Chuhong Fei, Deepa Kundur, and Raymond H. Kwong ," Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression "IEEE Transactions On Imageprocessing Vol.13, No. 2, Pp126-144,February 2004

[8] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "The effect of matching watermark and compression transforms in compressedcolor images," in Proc. IEEE Int. Conf. Image Processing, vol. 1, Oct. 1998, pp. 440–455.

[9] D. Kundur and D. Hatzinakos, "Mismatching perceptual models for effective watermarking in the presence of compression," in Proc. SPIE, Multimedia Systems and Application II, vol. 3845, A. G. Tescher, Ed.,Sept. 1999, pp. 29–42.

[10] M. Ramkumar and A. N. Akansu, "Theoretical capacity measures for data hiding in compressed images," in Proc. SPIE,Voice, Video and Data Communications, vol. 3528, Nov. 1998, pp. 482– 492.