INFORMATION SECURITY BY BIOMETRIC WATERKING

Kalpana Bhelotkar[1], Sandeep B. Patil[2]

1 Assistant Professor, ET & T Dept., C.I.T. Rajnandgaon, C.G., India, ***kal786bhelotkar@yahoo.co.in***
2 Sr. Associate Professor, ET & T Dept., SSCET Bhilai, C.G., India, ***patilsandeepb1212@rediffmail.com***

Abstract

In the recent digital world information security, person identification and authentication, and network security are the prime implications and off course requirements. To fulfill the above requirement watermarking is used widely with biometric information i.e. face image, iris, fingerprint, signature, hand geometry, voice and key stroke pattern. We propose a method for securing and protecting the biometric information of any person with the help of watermarking. The security can also be improved with the help of secrete key. Now a day's multimodal biometric watermarking is the most advanced technology for information security where more than one biometric information's are combined for enhancing security and privacy of information and system. In this paper we used face image as the biometric information to be secured, iris image with specific size with key is used for security improvement.

Index Terms: *Watermarking, Biometric, Biometric watermarking*

----------***----------

1. INTRODUCTION

Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity. A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina, and the one presented in this paper, the iris. Biometrics is based on using physiological, behavioral and chemical characteristics in personal identification and can easily separate an authorized person and a fake person.

Watermark is a digital code irremovably robustly and imperceptibly embedded in the host data and typically contains information about origin status and destination of the data . Although not directly used for copy protection, it can at least help identifying source and destination of multimedia data and as a "last line of deface" enable appropriate follow-up actions in case of suspected copyright violation.

Digital watermarking is a process in which an informed signal (watermark) is incorporated in multimedia content such as images to protect the owner's copyright over that content. The watermark can later be extracted from a suspected image and verified in order to identify the copyright owner. Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

One can classify digital watermarking in various categories, according to the visibility of watermark the digital watermarking is classified as: (1) Visible digital watermarking, (2) Invisible digital watermarking.

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It is also possible to use hidden embedded information as a means of covert communication between individuals.

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source

of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

2. PROPOSED METHOD

Watermark Is:
a) Data added to and often hidden within a media file.
b) Usually a small amount of data, often just a unique identification number.
c) Very hard to remove by distorting the Image.
d)Difficult to find if you don't know the Secret key.
e) Typically the same data repeated in every Video frame.
With the help of the biometric information (i.e. iris) and the secret key known by the person who wants to transmit the data can send the information as shown in fig -1.

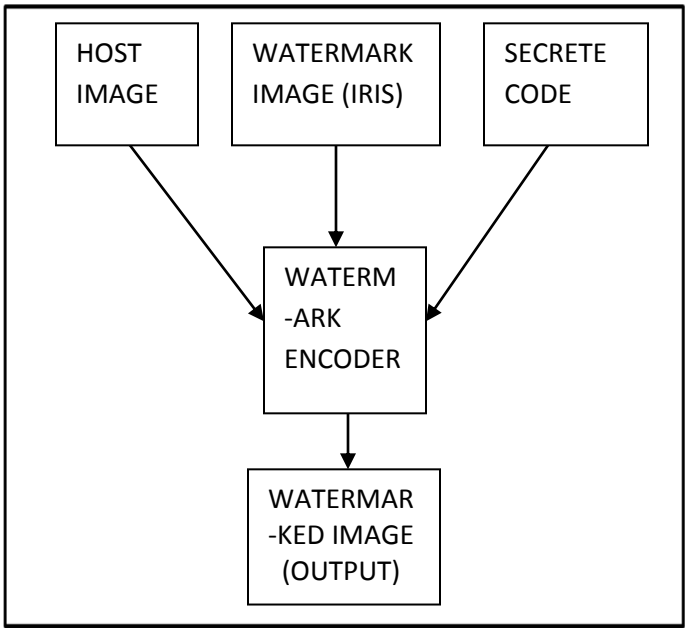

Fig -1: Watermarked image generation

At destination receiver get the watermarked image, for recovering the original image (information) he has to know the secret code it can be any alpha numeric code of larger size so that it cannot be easily cracked or hacked and watermarked image otherwise it will not be possible to get the original image or information as shown in fig -2.

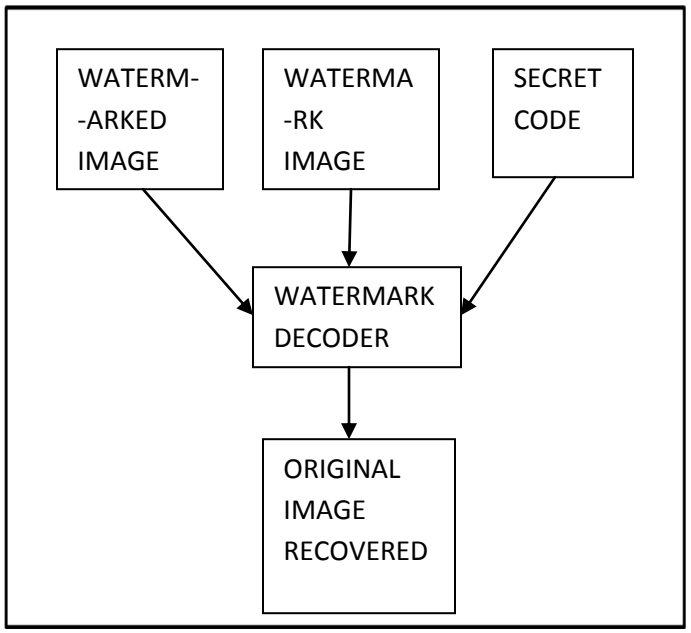

Fig -2: Original image reception at destination

CONCLUSIONS

The proposed method is much more simpler and provide high security to information transmitted from the insecure system or medium .One cannot easily excess the information until secrete code and watermarked information are not known. Here the code size is taken larger so guessing of code is tedious.

Finally we conclude that the proposed method is strong and can bear certain types of attacks. The ability of biometric based identification methods can distinguish between an authorized person and a fake person who fraudulently acquire the access privilege of an authorized person is one of the main reasons for their popularity compared to conventional methods. However security is an important issue. Watermarking and stenography are only solutions to prevent from fake persons.

FUTURE EXPANSSION

Multimodal biometric system can be employed here to improve the security with addition of code. More than one code can be used simultaneously.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their helpful suggestions. Kalpana would also like to take this opportunity to thank Mr. Sandeep B.Patil for his kind guidance during his study at the SSCET Bhilai when studying in ME.

REFERENCES:

[1]. Sanderson S., Erbetta J. Authentication for secure environments based on iris scanning technology. IEE Colloquium on Visual Biometrics, 2000.
[2]. A. K. Jain, Patrick Flynn, Arun A.Ross. "Handbook of Biometrics".
[3]. Seshadri R., Avulapati Y. K., Concealing the level-3 features of fingerprint in a facial image. IJCSE Vol.02, No.08, 2010, p.p. 2742-2744.
[4]. Paul P.P., Monwar Md.M., Human iris recognition for biometric identification IEEE 2007.

BIOGRAPHIES:

Kalpana Bhelotkar received the B.E. from RGPV Bhopal University, M.P., in 2003, pursuing Masters in Engineering in SSCET Bhilai. Her research interests include digital image processing, digital watermarking, and other communication related areas.

Prof. Sandeep B. Patil Associate professor in SSCET Bhilai, a renounced college in C.G. published numerous papers in various national and international generals and given guidance to number of students in different fields in electronics and telecommunication and pursuing PhD from CSVTU Bhilai.