Implementation of Image Authentication using Watermarking with Biometric Application

Meenakshi Shrawgi[1], Praveena Rajput[2]

[1] Research Scholar, Chouksey Engineering College, Bilaspur (C.G), India
[2] Associated professor ITGGDU, Bilspur (C.G),India

Abstract- This paper presents a secure watermarking scheme that inserts biometric data into images found in forms of identification. Putting biometric data deals privacy related issues. Here we present a software approach to implement such type of idea or giving a basic platform to implement it onto the further high level. Our process is the combination of two techniques: watermarking and biometric application. Watermarking is used for data security and biometric deals with unique identification. The paper is implementation of such type of approaches to fulfill the requirement of security and authentication. The basic concepts, implementation method, watermark insertion, watermark extraction process are given below. We take an image as an example to more understand the process . the summarized table with the performance parameters are also given.

Index Terms- watermark, biometric symbol like fingerprint, scanners, image sensor, comes sensor, mixed signal circuit.

I. INTRODUCTION

Watermarking is finding more and more support as a possible solution for the protection of intellectual property rights. A watermarking algorithm operates in many domains. The watermarking are of two types Visible and Invisible Watermarking. The use of both the techniques are depends upon particular application. Now for fulfilling the present requirement we can use some advanced technique like Data Encryption Standards (DES) and Advanced Encryption Standards (AES). The invisible watermarking with biometric application is described here.

A biometric is a measurement of a biological characteristic such as fingerprint, digital signature, iris pattern, retina image, face or hand geometry; or a behavioural characteristic such as voice, or signature. Biometric technology uses these characteristics to identify individuals automatically. Different biometrics will be more suitable for different applications. Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. It has a number of current and potential applications relating to national security and law enforcement.

II. MOTIVATION AND PROPOSED WORK

There are lot of ideas were implemented in the field of image security. But they are not too appropriate to fulfil all the requirements. We have a very nice and reliable method of security is encryption. But it is not appropriate for image security. We know that encryption changes the whole form of the data and converted it into some different form. In other words we can say that there is total conversion of the host data. The encryption is suitable for the data security because in the case of data we don't have any attention to make the original form instead we are interested to make it secure and vulnerable for theft so we choose encryption process. But when we are dealing with the image then our prime attention is to maintain the original data same as the host one. Because the images are the combination of the pixels arranged in the proper manner so when we apply the encryption algorithm on the images then the pattern will be changed and the original information contains on the image is not properly maintained. Hence we can say that for the data security we can apply the image encryption algorithm where we don't mean about the original shape and physical characteristics but for the images we employing the watermarking to maintain the watermark image same as the host image. When we considering the images then we have to maintain the image in proper sequence rearrangement of the image is somewhat difficult process. So to avoid this difficulty we use watermarking instead of encryption in which there is no intermediate conversion. For providing the unique authentication we are using the biometric applications as the keys which having some unique features to avoid the possibilities of data retrieving by unauthorised party.

III. IMPLEMENTATION PROCESS

The process has following three steps:

1. Watermark insertion
2. Watermark extraction
3. Watermark ASCII

3.1 WATERMARK INSERTION PROCESS

It is also called the encoding step in which we insert the watermark data into the host one in the form of biometric application for the security purpose. The attractive feature of the watermarking is that the host data is in the same form there is no intermediate conversion between them. Now after applying the watermark algorithm on to the host image we get the watermarked image which is the combination of the host image and the watermarking data (biometric data) but the we cannot differentiate the original image and the watermarked image they seems to be similar. The block diagram of the watermark insertion process is shown in fig 1. To more understand the

functioning the watermark steps for insertion and watermark flow chart is shown in fig 3 and fig 5 respectively.

3.2 WATERMARK EXTRACTION:

In the watermark extraction process we have to recovered the original image from the watermarked image in other words we have to extract the watermark biometric data if it is recovered same as the original one then the process is successfully completed on we get the matched output . If there is any mismatches then it is not possible to extract the original signal the original data and the watermarked data are stored in two different file Format to differentiate them easily. We apply the public key to the watermarked image and after applying the watermark extraction algorithm we got the original image. The block diagram steps and flow chart for the watermark extraction process are shown in fig 1, fig 3 and fig 5 respectively.

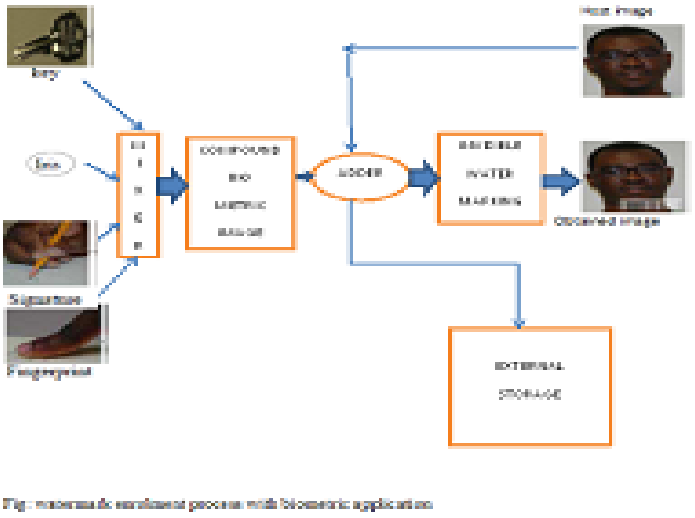

Fig 1: watermark insertion process

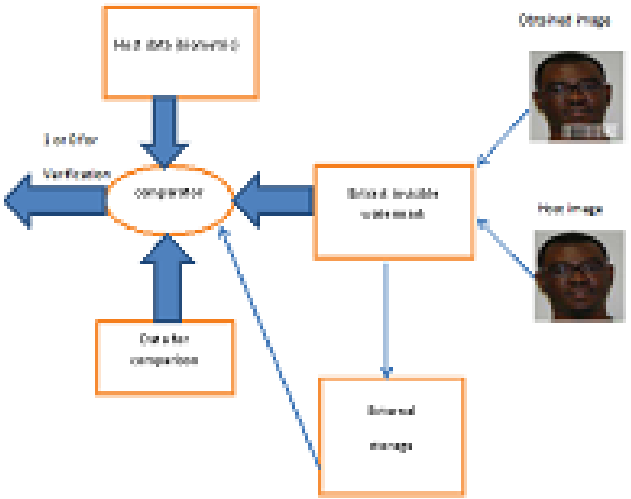

Fig 2: watermark extraction process

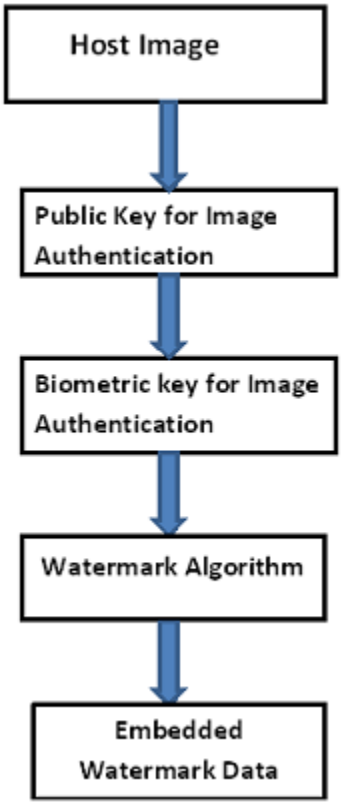

Fig 3: steps in watermark insertion process

IV. RESULT AND DISCUSSION

We are dealing with two methods the watermarking and the biometric applications for high level of security and authentication. This can be implemented by using MATLAB. To more understand the method we are considering an example of taking an image which has to be watermarked. Now a host image is shown in fig in which we are applying the watermarking algorithm using biometric key. The combined watermarked image with the biometric application is obtained. Image security and authentication both are provided. The biometric data provides us the uniform key which is added to the host data in such a way that the watermark should be transparent to users. We are using the invisible watermarking; no one can differentiate between the host image and the watermark image. They seem to be very similar we cannot differentiate them. It is the type of invisible watermarking in which we are using a fingerprint as a biometric key. When we extract the watermark then we get the fingerprint as the extracted key. The input image sail.png is applying with several biometric keys the various results are shown in fig. the various biometric keys are like fingerprints , hand signature and iris scans.

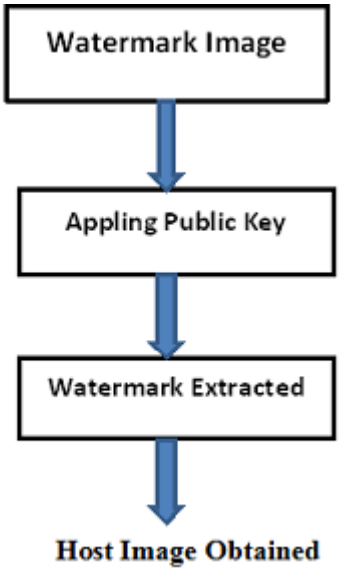

Fig 4: steps in watermark extraction process

V. CONCLUSION

The implementation of the proposed work is very simple and does not need any complex programming. There are many advantages like it provides us very reliable and secure approach for image security and authentication .It is a very unique method because it uses the biometric application as a main watermark key and as we know that the biometric symbols have the unique property because information which is transmitted is must accessed by the person having the unique identification (biometric key), The insertion and extraction of the keys are also very easy. The main feature of the proposed algorithm is that it is a very robust approach for image security the images/data are resistive and immune to noise .The insertion of the watermark data into the host data are provided in such a manner that the watermark should be transparent to us. We cannot see it but if someone want to access the watermark restrict its operation or any change.

The watermark can be scrambled through a well-known PN-sequence.. We can use AES and DES algorithms to make the keys more secure. The keys can be mixed into the host data by following the various algorithms. We can achieve high level security by using critical biometric symbols like DNA, BLOOD GROUPS, and SKIN TISSUES etc.

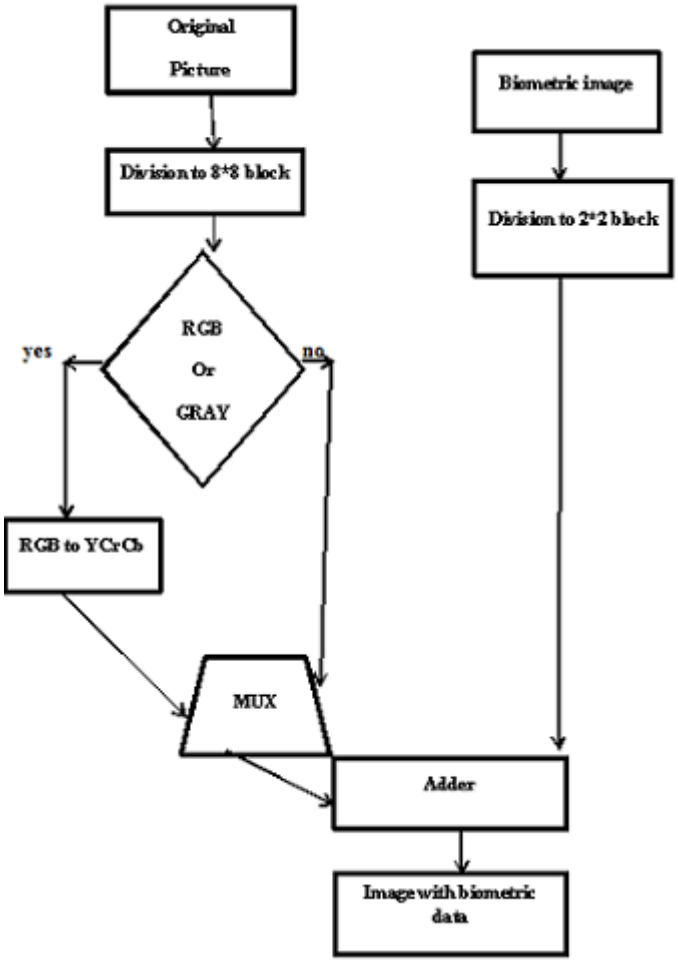

Fig 5: flow chart for invisible watermarking insertion algorithm

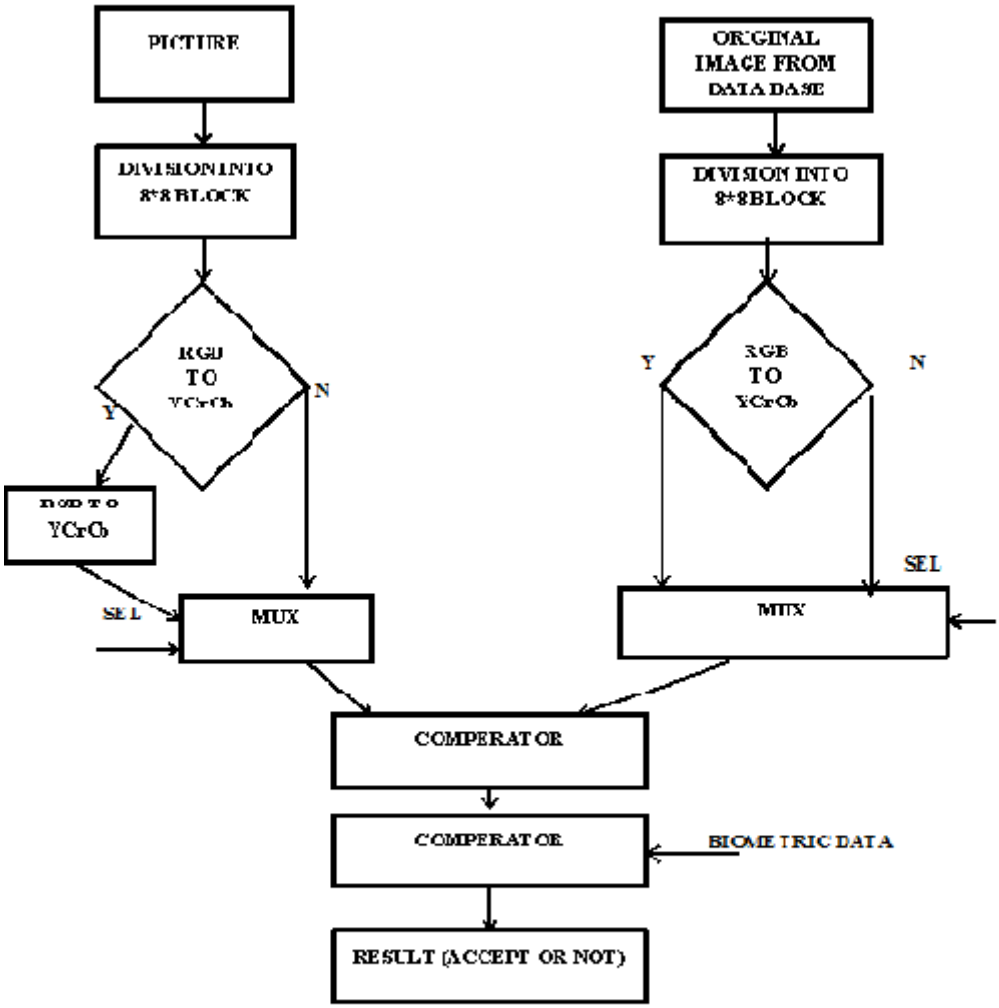

Fig 6: invisible watermarking extraction process

Figure (a)

Figure (c)

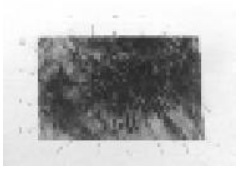

Figure (b)

Figure (d)

Fig 7: (a) original image, (b) fingerprint biometric key, (c) watermarked image, (d) extracted key

Figure (a)

Figure (c)

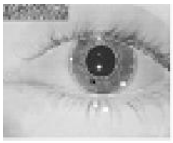

Figure (b)

Figure (d)

Fig 8: (a) original image, (b) iris biometric key, (c) watermarked key, (d) extracted biometric key

Figure (a)

Figure (c)

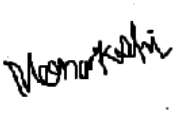

Figure (b)

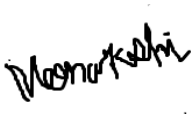

Figure (d)

Fig 9: (a) original image, (b) signature biometric key, (c) watermarked image, (d) extracted key

Table 1- Experiment with "Sail.Png" Original Image

S.NO.	PARAMETERS	BIOMETRIC FINGERPRINT KEY	BIOMETRIC IRIS KEY	BIOMETRIC SIGNATURE KEY
1.	ROBUSTNESS	GOOD	GOOD	GOOD
2.	AUTHENTICATION	EXCELENT	EXCELENT	EXCELENT
3.	UNIQUENESS	OPTIMUM	OPTIMUM	OPTIMUM
4.	CLARITY	VERY GOOD	VERY GOOD	VERY GOOD
5.	TRANSPERANCY	VERY GOOD	VERY GOOD	VERY GOOD

6.	SECURITY	GOOD	GOOD	GOOD
7.	GEOMETRIC DISTORTION	NO	NO	NO
8.	TRANSFERABLE	NO	NO	NO

REFERENCES

[1] Meenakshi shrawgi, Praveena Rajput, " Image Security and Authentication using Watermarking with Biometric application. M.tech. Digital electronics, December 2011 IEEE INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND COMPUTING RESEARCH ICCIC at kanyakumari ". IEEE Catalogue NO. CFP1120J-PRT ISBN:978-1-61284 -766-5/11/$26.00.

[2] Adamo, Oluwayomi Bamidele," VLSI Architecture and FPGA Prototyping of a Secure Digital Camera for Biometric Application". Master of Science (Computer Engineering), August 2006, 54 pp., 4 tables, 46 illustrations, references, 52 titles. IEEE 2006

[3] S.P. Mohanty, N.Ranganathan, and R.K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera Design", IEEE Transactions on VLSI Systems 13 (2005), no. 7, 808{818}.

[4] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kanakahalli, "A DCT Domain Visible Watermarking Technique for Images", Proceedings of IEEE International Conference on Multimedia and expo, 2000, pp. 1029{1032}.

[5] Lossless Visible Water Marking by using Translucent & Opaque Monochrome Methods IJCST Vol. 2, SP 1, December 2011 ISSN : 0976-8491(Online) | ISSN : 2229-4333(Print) .

[6] Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks ACM Journal Name, Vol. V, No. N, February 2008.

[7] S. Okada, S.I. Okada, Y. Matsuda, T. Yamada, and A. Kobayashi, 'System On A Chip For Digital Still Camera", IEEE Transactions on Consumer Electronics 45, no. 3, 9{12}.

[8] Robust image adaptive watermarking using fuzzy logic an fpga approach International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 3, No. 4, December, 2010

AUTHORS

First Author – Meenakshi Shrawgi, Research Scholar, Chouksey Engineering College, Bilaspur (C.G), India, Email: meenakshishrawgi@yahoo.com
Second Author – Praveena Rajput, Associated professor ITGGDU, Bilspur (C.G),India, Email: praveena.rajput@gmail.com