INTEGRITY CHECK IN BIOMETRIC IMAGE

Vishal Choudhary
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, U.P, India.
choudharyvishal@akgec.ac.in

***Abstract*— In today's technologically advanced world, the validity and reliability of biometric data are crucial for information exchange through erroneous networks as well as for the storage and management of massive data sets.To achieve previously mentioned, a watermark containing subtleties of proprietorship can be implanted in the biometric picture. Further, it is expected that the changed information can be turned around back to unique information with no data misfortune, once the subtleties have been retrieved. This study offers a fully reversible data watermarking methodology to prevent data gaps and address concerns with biometric verification and trustworthiness. The proposed method extracts the bare minimum of highlights using the discrete cosine transform (DCT). A reliable key is created in light of the first image's highlights and watermark. This key should be able to remove the watermark from the edited image.**

***Keywords*—DCT; Reversible watermakarking; Blind; Biometric image**

I. INTRODUCTION

A reversible watermarking scheme is a process whereby an original document may be marked with a message that can be easily removed. On the other hand, the process of removing this message may leave behind an unwanted mark or change in the content of the document. Some reversible watermark schemes suggest that it is possible to remove any mark without causing the loss of any text or other information contained within. By using reversible watermarking, it is possible to track the origin of a document and use the information so gathered for authentication purposes. Reversible watermarking can be used for authentication, content monitoring, management, and data storage.

The most common reversible watermarking schemes are shown in Figure 1. Additional types of reversible watermarks are shown in Figur 3. The schemes differ in how the marks themselves change or remain unchanged from the original mark (for example, from white to black). In reversible schemes, the message is contained within the original document and does not need to be separately stored.

The concept of reversible watermarking has been around for many years, with some companies claiming that they have been providing this service since the late 1980s. The first paper on this subject was presented by Petros Kokotas in 1991. Very few papers and patents have appeared since then.

There are several reasons why they may be not more popular: Adding a watermark to an image can be achieved using various techniques. For example, one might use a noise function that is added to the image. This can be either an independent random process or some information derived from the image itself. In this way, since the noise acts differently each time it is used, it will leave no discernible pattern in the image. It is also possible to add this noise in order to encode a binary message in the image using a frequency-hopping scheme.
Another method for adding a watermark uses some statistical properties of natural images (those without any signals added) in order to induce semantically meaningful patterns into them that act as watermarks.

II. PROPOSED METHOLODGY

Biometric images have been used as the host image in the suggested work. The suggested technique is divided into two phases: Procedures [A] for embedding and [B] for extracting data The biometric image is transformed using discrete cosines, and then the high recurrence region of the image is extracted. The primary justification for using the high recurrence component of the discrete cosine transform is that it more accurately represents the analogous signal in the discrete domain, which is where the majority of the biometric picture can be found. The embedding and extraction process is described in the following steps:

A. Embedding Procedure

After applying the DCT to the host image in the watermark implanting approach, highlights from the biometric images have been eliminated. In the suggested work, the biometric image is first subjected to Discrete Cosine Transform, after which the high recurrence portion is divided into blocks of s s size. The watermark is then added to the host image by altering each block's focal pixel value and comparing it to the watermark image's pixel value. The system for implanting

a watermark step-by-step is as follows: Take the biometric palm image B and use DCT to extract the high frequency component.

1. These low recurrence parts are separated into blocks Si of size s*s where I = 1, 2, ..., M
   M signifies the number of pieces in the watermark
2. Read the watermark picture P and apply scrambling calculation on P
3. Matrix P is changed over into the line vector
4. Now, altering the focal pixel worth of non-covering blocks to implant the watermark as follows:
   If Pi == 0 && (Central pixel value (I) %2)! = 0
   Then Si (k+1, l+1) = Si (k+1, l+1) + 1
   If Pi == 1 && (Central pixel value(I)%2)! = 1
   Then, at that point, Si (k+1, l+1) = Si (k+1, l+1) + 1
   Where k and l are the column and segment factors of block
5. Then watermarked biometric picture B* is obtained by applying IDCT.

The changed focal pixel of the watermarked picture is put away in a framework which is called as key and will be utilized for the recovery of the cover picture in the extraction cycle. Key size will rely upon the non-covering number of blocks and watermark size.

Figure 1 shows the stream outline of watermark installing technique according to proposed calculation.

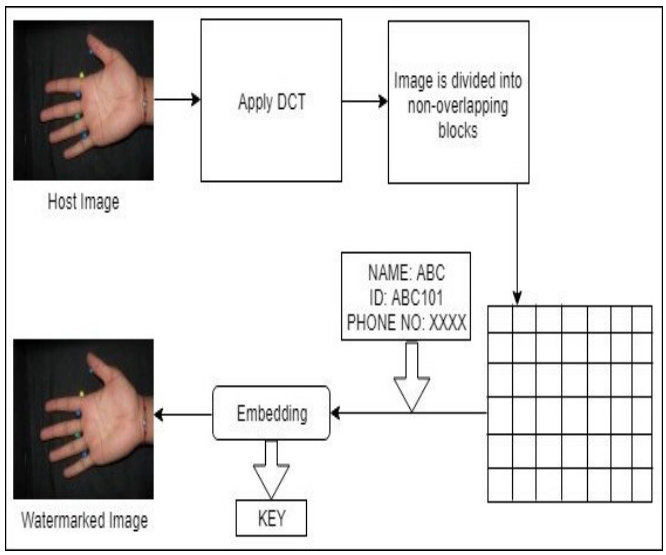

Fig.1 : Flowchart for Watermark Embedding

A. Extraction Procedure

The embedded watermark is taken from the watermarked image during the watermark extraction procedure. This approach is blind because the original cover picture and watermark are not necessary for watermark extraction at the receiving end. The following is a description of the stepwise watermark extraction process:

1. Apply DCT on the watermarked host image B*
2. Then high-frequency component of B* is partitioned into non-overlapping blocks of size Si where I = 1, 2, ..., M
   M denotes the number of bits in the watermark
3. Extraction of watermark bits from each non-overlapping block as follows:

   If Si (k+1, l+1) %2 == 0
   Then.set Pi to 0
   Else if. Si (k+1, l+1) %2 == 1
   Then set Pi to 1.
4. Then the extracted watermark is reshaped and de-scrambled to obtain the final watermark.
5. Now, read the key obtained in the embedding procedure and modify the central pixel value of watermarked image B* of each block with respect to the key and perform IDWT to obtain host image.

Below Figure 2 shows the picture representation of watermark extraction procedure

Fig.2: Flowchart for Watermark Extraction

EXPERIMENTAL RESULT

in this In this segment, the trial results of the proposed calculation are introduced. A few biometric palm pictures has been utilized in the trial and error. After some pre-handling on the dataset, palm pictures in jpg design changed over into BMP design. The presentation of the proposed calculation has been checked through Peak Signal to Noise Ratio and Normalized Correlation. The exploratory upsides of the accompanying variables are made sense of beneath: Peak signal to noise ratio (PSNR)

The quantitative evaluation of error between the original image and the modified image may be estimated using [1] by treating the original image and the modified image as signal and noise, respectively.

$$PSNR = 20log\,PSNR = 20log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \quad [1]$$

From [2] MSE (mean square method) can be calculated:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}||f(i,j) - g(i,j)||^2 \quad [2]$$

Where f is the original image matrix and g is the updated image matrix, I and j are the indices of the row and column, respectively, and m and n are the number of rows and columns, respectively.

Two photos are identical if the MSE between them is 0. Higher PSNR values indicate that the modified image is closer to the original than lower PSNR values do.

Table 1 PSNR of randomly selected 15 biometric images

#Sample Biometric Image	PSNR values
Image 1	55.96
Image 2	54.09
Image 3	52.03
Image 4	53.84
Image 5	52.90
Image 6	57.20
Image 7	58.32
Image 8	50.08
Image 9	59.03
Image 10	51.45
Image 11	55.34
Image 12	53.98
Image 13	52.04
Image 14	51.67
Image 15	53.88

The computed value of PSNR is shown in table I

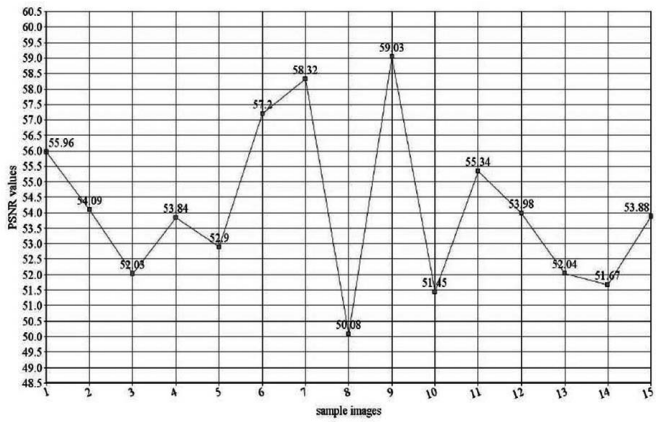

Fig. 3: Graphical Representation of PSNR values

The PSNR of 15 randomly chosen sample images used in experiments is represented graphically in Figure 3 and ranges from 50 to 59. It is obvious that this result is high when compared to the previous work.*Normalized Correlation*

NC determines the degree of similarity between an embedded and an extracted watermark. Let's assume that p is the watermark's size and that m and m' stand for the original and embedded watermarks, respectively. The NC can then be determined using [3]:

$$NC(M, M^{`}) = \frac{\sum_{i=1}^{p} \sum_{j=1}^{r} [M(i,j).M'(i,j)]}{\sum_{i=1}^{p} \sum_{j=1}^{r} [M(i,j)]^2} \quad [3]$$

When NC equals 1, it denotes that the extracted and embedded watermarks are mutually exclusive, but when it equals 0, it denotes that the hidden and retrieved watermarks are identical. Table II performance of Normalized Correlation

#Sample Biometric Image	Normalized Correlation
Image 1	1
Image 2	1
Image 3	1
Image 4	1
Image 5	1
Image 6	1
Image 7	1
Image 8	1
Image 9	1
Image 10	1
Image 11	1
Image 12	1
Image 13	1
Image 14	1
Image 15	1

Table II displays the NC and BER values that were calculated. Since the host image is not under attack, it is seen that the value of NC is 1. This demonstrates the algorithm's losslessness since the extracted and implanted watermarks are identical. different attacks on the proposed Algorithm

Attack	Normalized Correlation
Image 1	
No attack	1
Histogram Equalization	0.8328
Salt and pepper Noise	0.8792
Contrast Enhancement	0.8790
Gaussian Noise	0.8634
Image 2	
No attack	1
Gaussian Noise	0.8724
Contrast Enhancement	0.8707
Salt and pepper Noise	0.8645
Histogram Equalization	0.8863
Image 3	
No attack	1
Gaussian Noise	0.8890
Contrast Enhancement	0.8802
Salt and pepper Noise	0.8722
Histogram Equalization	0.8702
Image 4	
No attack	1
Gaussian Noise	0.8503
Contrast Enhancement	0.8730
Histogram Equalization	0.8678
Salt and pepper Noise	0.8636
Image 5	
Histogram Equalization	0.8792
No attack	1
Gaussian Noise	0.8834
Contrast Enhancement	0.8835
Salt and pepper Noise	0.8745

From the outcomes in desk III, it is able to be visible that during case of no assault the correlation price is 1 and greater than 0.86 whilst numerous assaults inclusive of Contrast Enhancement, Gaussian Noise, Histogram Equalization, and salt and pepper noise applied. It may be located that proposed technique is powerful in opposition to those assaults. comparison with the Existing Techniques:

Table IV: State of art table

	Type of host image	Data hiding method	PSNR Value	Correlation	Reversible/ non-reversible	Blind/ non-blind
Proposed algorithm	Biometric images	DCT	50.02-59.00	1	Reversible	blind
Biswas et al [21]	MRI, mammogram organ	Lossless and Data Compression	43.0897-45.4998	Not reported	Partially	Blind
Hawlader et al [18]	Medical images	DWT and chaotic system	45.09-48.99	1	Non-reversible	blind
Naheed et al [22]	MRI	GA and PSO	49.003748-49.011976	1	Reversible	Not reported
Subrato Bharati et al [4]	Medical images	DCT + BFO	48.66-49.69	Not reported	Not reported	Not reported
Rohit M. Thanki et al [3]	Digital Images	DCT-SVD	28.65-40.69	Not reported	Not reported	Not reported
Philip et al [20]	MRI	DWT-SVD	30-40	0.9821-0.9923	Non-reversible	Not reported

Table IV demonstrates that the suggested strategy led to superior results in terms of NC and PSNR values..

IV. CONCLUSION

The Proposed Approach Is Totally Reversible Watermarking Plan Without Any Deficiency Of Data And Takes Care Of The Issue Of Biometric Verification And Honesty Control. The Proposed Strategy Uses The Discrete Cosine Change (Dct) For Minimized Highlights Extraction And In View Of The Component Extricated From The First Picture And Watermark, A Key Is Created. It Gives A Protected Computerized Watermarking Plan For Biometric Palm Pictures Which Is Hearty Towards The Mistakes/Twists In The Pictures Emerging Because Of The Blemishes During The Capacity, Handling In Huge Data Sets And Transmission In Wrong Correspondence Organizations. The Registered Worth of Nc is 1 and the Worth of Psnr is over 50, which clearly shows that the proposed calculation is lossless in nature because the extricated watermark is the exact same as the implanted watermark, according to the trial and error.

REFERENCES

[1] Dey, N., Biswas, D., Bardhan, A., Das, R.A. and Chaudhuri, S.S., "DWT DCT SVD based blind watermarking technique of gray image in electrooculogram signal", IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp.680–685, 2012.

[2] Kumar, E.P., Philip, R.E., Kumar, P.S. and Sumithra, M.G.,"DWT-SVD based reversible watermarking algorithm for embedding the secret data in medical images", Fourth IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp.1–7, 2013

[3] Thanki, R. M., & Kothari, A. M. (2019). Hybrid domain watermarking technique for copyright protection of images using speech watermarks. Journal of Ambient Intelligence and Humanized Computing.

[4] Bharati, S., Rahman, M. A., Mandal, S., & Podder, P. (2018). Analysis of DWT, DCT, BFO & PBFO Algorithm for the Purpose of Medical Image Watermarking. 2018 International Conference on Innovation in Engineering and Technology (ICIET).

[5] Ali Z., Imran M., Alsulaiman M., Zia T., Shoaib M., "A zero-watermarking algorithm for privacy protection in biomedical signals" Future Generation Computer Systems, 82 , pp. 290-303, 2018.

[6] M. Mishra, A. Bhattacharya, A. Singh and M. K. Dutta, "A Lossless Model for Generation of Unique Digital Code for Identification of Biometric Images," 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2018, pp. 1-5.

[7] Rajabi M.J., Abdullah S.M., Bakhtiari M., Bakhtiari S. (2018) A Robust DCT Based Technique for Image Watermarking Against Cropping Attacks. In: Saeed F., Gazem N., Patnaik S., Saed Balaid A., Mohammed F. (eds) Recent Trends in Information and Communication Technology. IRICT 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 5. Springer, Cham

[8] A. Singh, N. Raghuvanshi, M. K. Dutta, R. Burget and J. Masek, "An SVD based zero watermarking scheme for authentication of medical images for tele-medicine applications," 2016 39th International Conference on Telecommunications and Signal Processing (TSP), Vienna, 2016, pp. 511-514

[9] W. Wójtowicz, M.R. Ogiela, Digital images authentication scheme based on bimodal biometric watermarking in an independent domain, J. Vis. Commun. Image Represent 38 (2016) 1–10

[10] G. Balamurugan and M. Senthil, "A fingerprint based reversible watermarking system for the security of medical information," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-6.

[11] H. B. Kekre, T. Sarode and S. Natu, "Biometric watermarking using partial DCT-Walsh wavelet and SVD," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 124-129.

[12] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak [a]Audio Watermarking Using Pseudorandom Sequences Based on Biometric Templates[o]- Journal of Computers, Vol. 5, No. 3, 2010, pp. 372-379.

[13] T. Ignatenko and F.M.J. Willems, "Biometric Systems: Privacy and Secrecy Aspects", IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, Pp. 956 – 973, 2009.

[14] Lifang Wu, Xingsheng Liu, Songlong Yuan and Peng Xiao, "A novel key generation cryptosystem based on face features", IEEE 10th International Conference on Signal Processing (ICSP), Pp. 1675 – 1678, 2010.

[15] J.G. Jo, J.W. Seo, and H.W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop, Pp. 38-49, Springer Verlag, 2007.

[16] Feng Wen-ge, Liu Lei, "SVD and DWT Zero-bit Watermarking Algorithm", 2nd International Asia Conference on Informatics in Control, Automation and Robotics, pp. 361-364, 2010.

[17] Chunhua Dong, Jingbing Li, Huaiqiang Zhang, Yen-wei Chen,

"Robust Zero-Water-marking for Medical Image Based on DCT", 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp. 900-904, 2011.

[18] Moniruzzaman, M., Hawlader, M.A.K. and Hossain, M.F. (2014) 'Wavelet based watermarking approach of hiding patient information in medical image for medical image authentication', 17th International Conference on Computer and Information Technology (ICCIT),pp.374–378.

[19] Dey, N., Biswas, D., Bardhan, A., Das, R.A. and Chaudhuri, S.S. (2012) 'DWT DCT SVD based blind watermarking technique of gray image in electrooculogram signal', IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp.680–685.

[20] Kumar, E.P., Philip, R.E., Kumar, P.S. and Sumithra, M.G. (2013) 'DWT-SVD based reversible watermarking algorithm for embedding the secret data in medical images', Fourth IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp.1–7.

[21] Dey, N., Biswas, D., Bardhan, A., Das, R.A. and Chaudhuri, S.S. (2012) 'DWT DCT SVD based blind watermarking technique of gray image in electrooculogram signal', IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp.680–685.

[22] Naheed, T., Usman, I., Khan, T.M., Dar, A.H. and Shafique, M.F. (2014) 'Intelligent reversible watermarking technique in medical images using GA and PSO', Optik – International Journal for Light and Electron Optics, Vol. 125, No. 11, pp.2515–2525 [online] http://dx.doi.org/10.1016/j.ijleo.2013.10.124 (accessed 2 April 2015).

ABOUT THE AUTHOR

Vishal Choudhary is working as an Assistant Professor in the Department of Computer Science & Engineering, AKGEC Ghaziabad. He has completed his M.Tech from Centre for Advanced Studies, AKTU. He has several publications in various journals of repute.