Watermarking of digital images with iris based biometric data using wavelet and SVD

B.Alekya Hima bindu , V.Saraswati
Assistant Professor, ECE Dept., SREC , Nandyal, Kurnool (dist),Andhra Pradesh.
Assistant Professor, ECE Dept., RGMCET , Nandyal, Kurnool (dist),Andhra Pradesh

***Abstract* - Watermarking is the most smart and appropriate technique for copyright protection and security of multimedia data. Watermarking has been recommended for the civilizing security of biometric systems. Conversely Iris recognition is regard as the most trustworthy and exact biometric identification system accessible. This paper extracted iris feature using a novel grid based approach . The grid based watermarking algorithm uses a hybrid Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) and method. In this approach, the singular value of the original data has been modified using multiple scaling factors for embedding the watermark image. The Watermarked image obtained by the proposed approach is robust under various attacks such as rotation, cropping, JPEG compression, Histogram equalization, Average filtering and Gaussian noise. This method provides a scalable, secure, strong and undetectable form of watermarking. This proposed scheme minimizing fault acceptance rate and the fault error rate in very efficient manner.**

***Index terms* - Digital Watermarking, Singular Value Decomposition (SVD), biometric technology**

I. INTRODUCTION

The rapid development of the Internet and availability of networked computers has made the distribution of multimedia data very fast and convenient without losing information. The consequences of such applications lead to modification and distribution of illegal data easier for the unauthorized parties. To overcome these problems, digital watermarking technique came into existence. Digital watermarking is a technique of inserting copyright (watermark) into the digital data, such as text, audio, image and video, etc.

In visible watermarking, watermark is visible, because the watermark is overlaid on the original image. The watermark needs to be overlaid in a way that it has to be difficult to remove the watermark which can be a text or logo. In invisible watermarking the watermark is embedded imperceptibly into the original image. One of the simple invisible watermarking schemes is modifying the LSB plane of the original image with the message bits that need to be embedded.

Spatial domain watermarking is simple and has advantages of easy implementation, low complexity. In spatial domain watermarking, the embedded watermark can't resist image processing operations or attacks. The Frequency domain watermarking is performed by inserting the watermark into the magnitude of the coefficients in the frequency domain. Existing transform domain watermarking techniques include: FFT (Fast Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), SVD (Singular Value Decomposition) and hybrid (Combination of the above transforms).

In Transform domain watermarking techniques, DWT and SVD watermarking techniques have been proposed. DCT domain watermarking is classified into global and block-based DCT watermarking. In the global DCT scheme, a watermark is embedded in perceptually significant portion of the original image and the watermarking schemes based on DCT.A hybrid watermarking technique using a combination of both DWT and SVD transforms for user authentication in biometrics is proposed in. DWT and the SVD watermarking scheme is proposed.

DCT watermarking method for sub bands of a digital image has been proposed. In the DWT watermarking scheme, the watermarking method is same as in DCT, the difference is in the process of transforming the original image in its frequency domain. Different DWT watermarking schemes have been proposed. One of those is at multiple resolutions the watermark is embedded in all high pass bands in a nested manner.

There are various techniques of implementing transform domain watermarking like Fourier transform, discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) and many more. Here DWT- and SVD-based hybrid transform domain has been used. This is because the multi resolution property of DWT increases the imperceptibility, whereas SVD aids in improving the robustness of the scheme. Unlike the traditional methods of using an image or a random signal as a watermark, here the authentication information used as watermark is the iris biometric data of the user. It is used as the user id in this case, similar to various methods that use a logo as watermark. A biometric is based on the concept of 'something – you-are', so it increases the security criteria many folds in comparison to the traditional watermarking methods. Biometrics like iris, retinal scan, fingerprint scan, hand geometry, facial scan and so on carries the unique biological information about the user. Retinal scan is the most secure of these but it is not very user friendly, whereas facial scan, finger print and hand geometry are the most user-friendly but not as much secure as iris or retinal scan . Iris biometric gives an optimised option of user-friendly as well as secure biometric. This is because an iris image of a person can be collected from a distance of couple of meters unlike retinal scan, finger print or hand geometry. Moreover unlike fingerprint once a person is dead his pupils stop dilating so the iris scan of a

dead person does not match with a live one. Whereas in comparison to facial scan iris biometrics of twins are not same, and neither do they change with age like the human face.

II. WATERMARKING METHODOLOGY

The watermarking methodology of using hybrid format of the two robust techniques, that is discrete wavelet transform (DWT) and singular value decomposition (SVD) has been employed here. The idea of implementing both the technologies, that is, biometrics and watermarking has been done in two ways. The first, watermarking a biometric data, which is used as a host with a watermark, for protection of the integrity of the biometric data to enhance the security. Whereas the second is where the watermark is a biometric and is used for the authentication of the host image. Here the work is of the second type. Previously, researchers have used mainly fingerprint and face for this second type of watermarking a host image with a biometric for its protection .The method used is very simple taken from our previous work . However, out of the various multi-metric techniques proposed, the easiest and the one having lowest complexity, as well as time constraint with significant identification is proposed. The method can be implemented either row-wise or column-wise, in one-dimensional (1D)DCT of the intensities. This is done to obtain the DC coefficients after DCT to give a 1D sequence of DC values for the 2D greyscale iris biometric intensity image.
This 1D biometric data here is used as the watermark. The scheme employed here is similar on the lines of hybrid transform.

$$X_i^n(k, l) = w(k) \sum_{l=1}^{M} x(n, l) \cos \frac{(2l-1)(k-1)}{2M},$$

$$k = 1, 2, \ldots..M$$

The DCT of a row of the iris matrix is defined as,

where $x(n, l)$ is lth sample of the signal in the nth row of the ith iris image, M is the column size, and $w(k) = \sqrt{1/M}$ for $k = 1$ and $w(k) = \sqrt{2/M}$ for $2 < k < M$.

Where x(n,l) is the Lth sample of the signal in the nth row of the ith iris image, M is the column size, and w(k)=
The steps employed, as in Fig. 1, to obtain the iris biometric in 1D watermark format is as under:

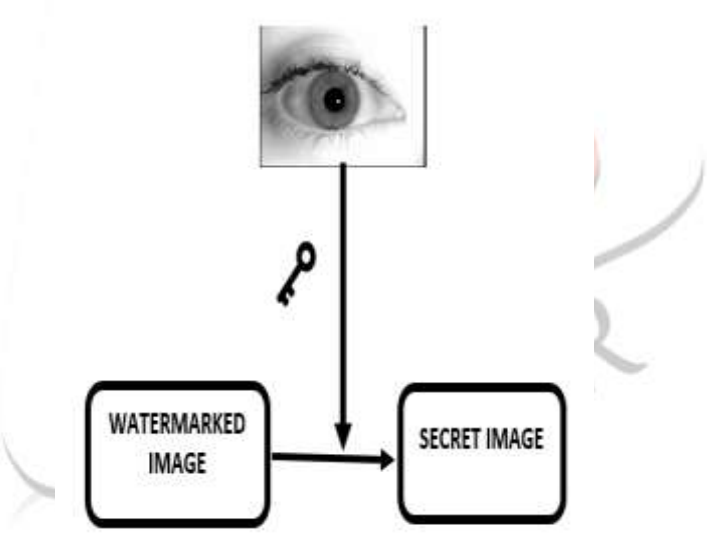

figure 1.:extraction process

The watermarked image is given as input
AUTHENTICATION FOR THE SECRET MESSAGE

- Give input eye image of a person and perform SURF operation
- Detect key points[1] from the image by calculating the orientation, descriptor &count
- Count displays the total number of features detected.
- The count value generated is used as a key for the authentication of the secret image.
- If the attached key is matched with the generated key, it confirms the authorization of that person.
- DWT is applied to it and is decomposed to its respective coefficients
- Re-construct the SVD matrix for each band, and extract the secret image.

III. BIOMETRIC TECHNOLOGY

The two major ways of doing watermark are spatial domain and the robust transform domain. In this study, method for watermarking of digital images, with biometric data is presented. The usage of biometric instead of the traditional watermark increases the security of the image data. The biometric used here is iris. This paper proposes a method to establish joint ownership of digital images by embedding imperceptible digital pattern in the image. This digital pattern is generated from biometric features of more than one subject in a strategic matter so that the identification of individual subject can be done and the multiple ownership of the digital images can be established. This digital pattern was embedded and extracted from the image and the experiments were also carried out when the image was subjected to signal processing attacks. Coefficients of mid frequency band

discrete cosine transform was used for embedding as these coefficients do not adversely affect the perceptual transparency and is also significantly robust to normal signal processing attacks. Experimental results indicate that the insertion of this digital pattern does not change the perceptual properties of the image and the pattern survives signal processing attacks which can be extracted for unique identification.

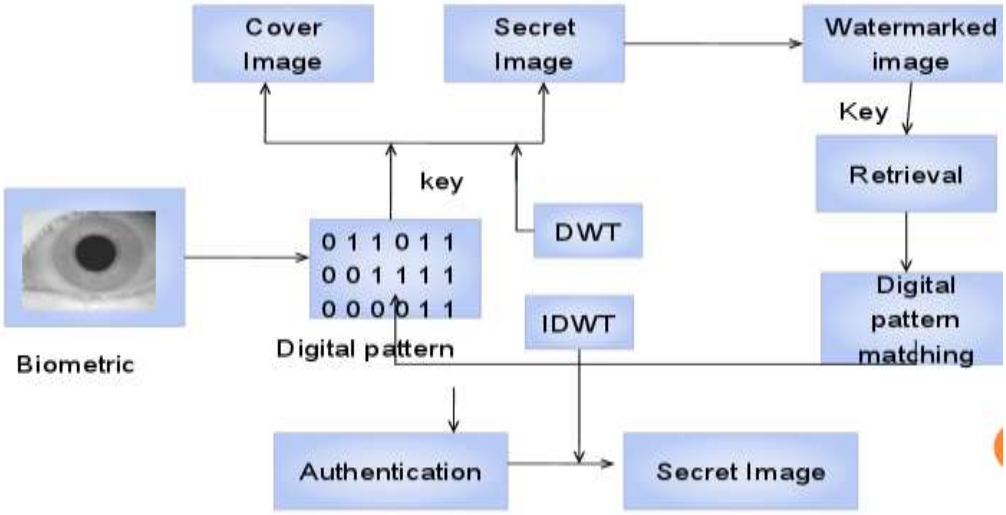

Figure2: Block Diagram

Wavelet Based Watermarking

Discrete Wavelet Transformation is the transformation which decomposes the original image into four frequency sub-bands which are LL, LH, HL and HH. LL is the lowest frequency level having approximation information; LH is the vertical information; HL is the horizontal information and HH is the diagonal information of an image. DWT has an advantage that any sub-band can further be decomposes into another sub-levels and can also be extended up to n-levels. Most of the approximation information is in the low frequency sub-band i.e. LL and other three high frequency components are having detailed information of an image like edge, textures etc. So, the watermark embedding is mostly done in LL sub-band as it is much more stable than higher sub-bands and gives better robust results.

Modified 2D discrete cosine transform based system

In this system the image is divided into 8×8 blocks and discrete cosine transform of the image is calculated on each blocks of image then find the lowest and highest frequency coefficient components of the image. so the DCT approaches for watermarking systems do not give some forms of attacks.

Redundant Discrete Wavelet Transform (RDWT) based watermarking system

Mostly the discrete wavelet transform is used in image watermarking because discrete wavelet transform gives frequency information in stable form and it allow good localization both in time and frequency domain. Conversely The DCT having one of the main demerits is that the transformation does not provide shift invariance because of the down sampling of its band. The shift variance of the DWT leads incorrect extraction of watermarking systems so we need to know the precise locations of where the watermark information is embedded so the small shift variance cause the wavelet coefficient of the input.

In this uses wavelet based watermarking techniques and it is based on the human visible system. The human visible system having the one essential characteristics that is Just Noticeable Profile (JND) which is used for watermark embedding to improve the imperceptibility of the system. First estimate the allowable visibility ranges of the JND threshold for all coefficient of the wavelet transformed image. The system deeds the range to calculate the adaptive strength to be covered in the wavelet coefficient while embedding watermark. Then the system exploits the artificial neural network which is used for remember the relationship between the original wavelet coefficients and its watermark version. During the extraction the trained artificial neural network used to calculate the watermark coefficient without use of the original image. It gives better performance compared to other watermarking systems.

The host image is applied with the single level DWT using Daubechies (N = 6) wavelet to obtain the four set of coefficients CA, CH, CV and CD. This is followed up by SVD operation on each of them on similar lines, to obtain the two orthogonal matrices U and V and the set of eigen values in S. For the band being CX (here as the same operation is repeated for the approximate band, that is, CA, horizontal band, that is, CH, vertical band, that is, CV and diagonal band, that is, CD the iterative method is referred as CX, that is, CA/CH/CV/CD) the operation is as in the following equation

$$CX = U \times S \times VT,\ CX = CA/CH/CV/C \qquad (1)$$

The iris biometric watermark is embedded in the eigen value matrix S to obtain S* with CRC200 being the CRC-based 200 DC values of the iris template in binary, as in (3). The CRC used is MATLABs inbuilt CRC-16 cyclic redundancy check codes . This CRC200 is divided by the threshold KEY; this is to reduce the payload of the embedded watermark (Fig. 2). Then SVD is again applied on the S* matrix to obtain S1, U1 and V1. Here too S1 is the Eigen value matrix.

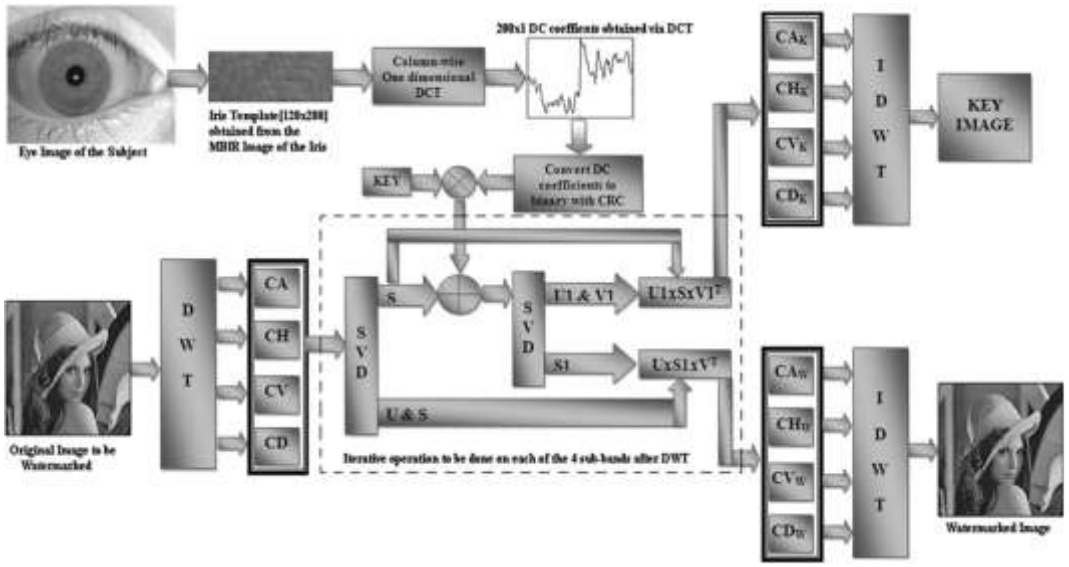

Figure3 : Iris biometric based image watermarking algorithm

of S*, whereas U1 and V1 are the orthogonal matrices. The CRC200 data are added to the modified Eigen value matrix in a linearised way

$$S0 = S1 + CRC200/KEY = U1 \times S \times V_1^T \quad (2)$$

Now the orthogonal matrices of first SVD operation, that is. U and V are combined with the Eigen values of the second SVD operation, that is S1 to obtained the subband for watermarked image, that is CW. The rest, that is U1 and V1 are combined with the Eigen values of the first SVD operation, S to obtain CK, the subband for the key image. Though they could be kept as key matrices instead it is preferred to keep them as 'key image' as this would require less memory inplace of keeping them as key matrices. In case there are no memory constraints they can be kept as key matrices and be used whereas extraction of the watermark (Fig. 3). Here the word 'key image' refers to the image required during the extraction procedure along with the corrupted image.

$$U \times S1 \times VT = CW, \; CW = CAW/CHW/CVW/CDW \quad (3)$$

$$U1 \times S \times VT1 = CK, \; CK = CAK/CHK/CVK/CDK \quad (4)$$

IV. SVD BASED WATERMARKING

The SVD based algorithms mostly used in image processing and visualization it operates only on a positive matrix. The cover image considered as a matrix then the cover image matrix divided into three sub matrix with singular value decomposition and watermark image added with cover image matrix it having the singular values and it will generate watermarked image. The decomposition technique is applied to the watermarked image. Finally the watermark image decoded from cover image using decomposition method. This system gives the very good image stability and intrinsic algebraic image properties.

In most of the image processing applications, image can be perceived as a matrix with non-negative scalar values. The SVD of an image F of size M x M is calculated as, F = U S VT, where U and V are orthogonal matrices of size M x M and M x M respectively, and S is a diagonal matrix of size M x M i.e., S = diag (ei) where ei 's are the singular values arranged in decreasing order with i = 1, 2, 3, ..., M. Singular values of an image will have most of the energy concentrated in the beginning of the diagonal matrix as they are arranged in decreasing order. It contains the luminance values of the image and the slight modification done to the singular values will not affect the original image visual quality. So, for SVD watermarking the singular values are used for embedding the watermark. SVD of image F can be written as:

$$F = \sum_{i=1}^{r} u_i \, s_i \, v_i^T \quad (5)$$

Here r specifies the rank of the matrix F, ui and vi are left and right singular vectors respectively. From [5], The SVD watermarking is as follows: First, the SVD operation is performed on the original image, F resulting in three matrices U, S and V. Then, a watermark is embedded in diagonal matrix, S as S' = S + α W, where α is used to scale the watermark strength and SVD operation is employed on S' obtain three matrices UW, SW and VW. The watermarked image, FW is obtained by multiplying three matrices U, SW and VT.

$$F = U \, S \, V^T;$$

$$S' = S + \alpha.W, \text{ where } \alpha.W \text{ is point wise multiplication, i.e., } \alpha \, W = (\alpha 1W1, \alpha 2W2, .. \, \alpha nWn)T;$$

$$S' = U_W \, S_W \, V_W^T;$$

$$F_W = U \, S_W \, V^T;$$

By performing the inverse operation of the watermarking, watermark extraction can be done. FW* is possibly modified watermarked image.

$$FW^* = U^* \, S_W^* \, V^{*T};$$

$$D^* = U_W \, S_W^* \, V_W^T;$$

$$W^* = (1/\alpha) \, (D^* - S); \quad (6)$$

The verification of the watermark can be done by correlating with the inserted watermark. The scaling vector α plays an important role in obtaining robustness. Choosing the optimal vector α using Brute-Force technique requires an exponential amount of time. Hence, it is better to use soft computing technique to find optimal or close to optimal in polynomial time. Genetic Algorithms (GA) to find optimal vector α to get best robustness. In this paper, we use Tabu Search to find optimal vector α and the experiment done on the standard data set shows that Tabu Search gives more robustness than the GA in watermarking.

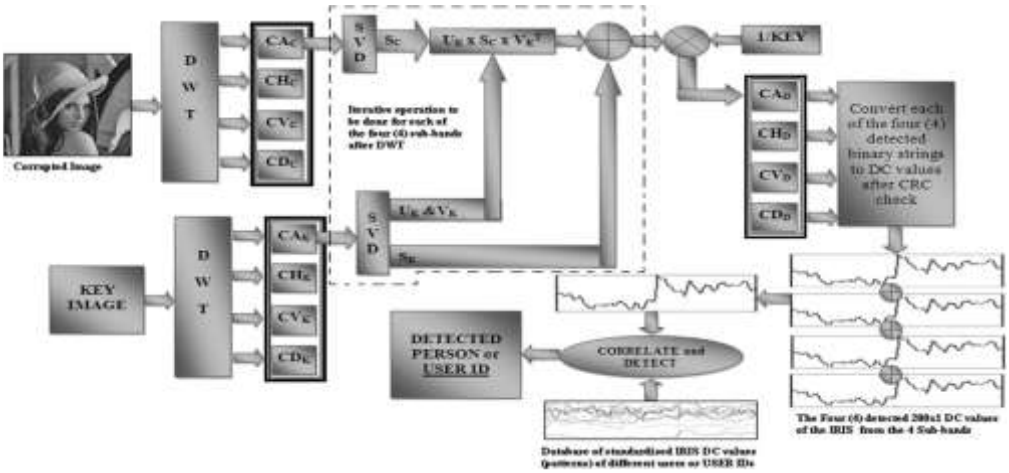

Figure4: Watermark extraction and biometric identification algorithm

These operations applied on all the four subbands, generate the four subbands for both key image and watermarked image. Then on application of the inverse discrete wavelet transform (IDWT) on the CAK, CHK, CVK and CDK generates the key image. Similarly, the watermarked image is generated on application of IDWT on CAW, CHW, CVW and CDW. For the extraction of the watermark from the stego image, the reverse of the above scheme is employed. Here the corrupted version of the watermarked image is considered to be received. Similar to the embedding process, the DWT of the image is taken to obtain the corrupted image's subbands CAC, CHC , CVC , and CDC. The image is decomposed back to its respective coefficients as well. Then on each respective subband pair of corrupted image and key image, the SVD is applied to obtain UC, SC, VC, UK, SK, and VK, respectively. The Eigen values of the stego image, SC are combined with the respective orthogonal matrices UK and VK of the key image to generate the stego subband matrix D as in (7). The Eigen values of the key image SK are then subtracted from the matrix D to obtain the watermark coefficients CXD for that particular subband after normalisation with the threshold named KEY, as in (8). This KEY was the multiplying factor applied to CRC DC coefficients to reduce the intensity in the embedding process.

$$D = UK \times SC \times V^{T}_{K} \quad (7)$$

$$CXD = (1/KEY) \times (D - S_K), \quad (8)$$

$$CXD = CAD/CHD/CVD/CDD \quad (9)$$

So from the obtained watermark coefficients CAD, CVD, CHD, and CDD the four sets of DC values of the iris biometric is obtained. This is done by firstly removing the CRC error control coding redundant bits, followed by conversion of the binary data to pixel intensities of the DC values. From the set of the four set of DC values detected from the four wavelet subbands a normalised set of DC coefficient is obtained. This obtained set of DC coefficient is correlated with the standard sets of DC coefficient stored for each person for detection, authentication and identification of the biometric watermark. Based on this biometric watermark the person identification or detection of the user id of the subscriber is obtained. This is done using the self-similarity patterns as per our previous work .There it was found that the DC coefficients follow a particular self-similarity pattern for every particular eye. Even the left and right eye of any particular person follows a different set of pattern.

V. RESULTS AND DISCUSSION

The technique employed has many factors that may affect the resulting watermarked image and the extracted watermark and its template matching with the signature data base. When the watermark is embedded in first level decomposition as coefficients are significant image gets more distorted and SNR and PSNR values are less compared to when embedded in second level. The correlation between extracted and the original watermark is almost equal trade-off has to be achieved among these two factors whereas distorted the watermarked image and the more time it takes to embedded the watermark. This technique work well with watermark that include fewer black area.

VI. CONCLUSION

A digital image watermarking scheme based on SVD has been proposed in this paper. Multiple scaling factors are used to embed the watermark in the diagonal matrix instead of one constant value.. The proposed method performs successfully during the attacks and the watermark can be extracted with very less degradation. During the attacks, the correlation between the extracted and inserted watermark is closer to 1 (means similar) and it performs better than the other similar works. It is observed that the proposed method is more robust compared to the algorithm that used Genetic algorithm for finding optimal scaling factors.

A non-blind approach of integrating the highly secure iris biometric has been integrated with the image watermarking algorithm to enhance multimedia security of data. The algorithm here for the biometric generation has been kept very simple to reduce

complexity of implementation. Moreover the integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. Thus this scheme provides a secure robust- imperceptible watermarking technology in total.

VII. REFERENCES

[1] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain" IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.
[2] P. L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," Pattern Recognition, vol. 38, no. 12, pp. 2519–2529, 2005.
[2] Gupta, Manish, et al. "Digital image watermarking using uncorrelated color space." *Proceeding of International Symposium on. Computer Applications and Industrial Electronics (ISCAIE)*, IEEE, 2014:158-162.
[3] Abdullatif, Mohammad, et al. "Properties of digital image watermarking."*Proceeding of 9th International Colloquium on Signal Processing and its Applications (CSPA)*, IEEE, 2013:235-240.
[4] Majumder, Swanirbhar, KharibamJilenkumari Devi, and Subir Kumar Sarkar. "Singular value decomposition and wavelet-based iris biometric watermarking." *Biometrics, IET* 2.1 (2013): 21-27.
[5] Franklin, Rajkumar V., Manekandan GRS, and V. Santhi. "Entropy based robust watermarking scheme using Hadamard transformation technique."*International Journal of Computer Applications* 12.9 (2011): 14-21.
[6] Khalili, Mehdi, and David Asatryan. "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map." *IET Signal Processing* 7.3 (2013): 177-187.
[7] Pradhan, Chittaranjan, Vilakshan Saxena, and Ajay Kumar Bisoi. "Imperceptible watermarking technique using Arnold's transform and cross chaos map in DCT domain." *International Journal of Computer Applications*55.15 (2012).
[8] Katzenbeisser, S., Petitcolas, F.A.P.: 'Information hiding techniques for steganography and digital watermarking' (Artech house, Computer
security series, 2000), pp. 15–23, 97–109.
[9] Liu, R., Tan, T.: 'A SVD-based watermarking scheme for protecting rightful ownership', IEEE Trans. Multimedia, 2002, 4, pp. 121–128 3 Johnson, N.F., Duric, Z., Jajodia, S.: 'Information hiding, steganography' (Kluwer Academic Publisher, 2003), pp. 15–29.
[10] Mallat, S.: 'A theory for multiresolution signal decomposition: the wavelet representation', IEEE Trans. Pattern Anal. Mach. Intell., 1989, 11, pp. 674–693.
[11] Zhu, X., Zhao, J., Xu, H.: 'A digital watermarking algorithm and implementation based on improved SVD watermarking-attacks and counter measures'. Proc. 18th IEEE Computer Society Int. Conf. Pattern Recognition (ICPR'06).
[12] Daugman, J.: 'How iris recognition works'. Proc. of 2002 Int. Conf. on Image Processing, 2002, vol. 1.
[13] Wildes, R., Asmuth, J., Green, G., et al: 'A system for automated iris recognition'. Proc. IEEE Workshop on Applications of Computer Vision, Sarasota, FL, 1994, pp. 121–128.