Fragile Water-Marking Based Image Authentication Scheme using LSBs

Sandeep Kaur, Alka Jindal

Abstract*: *This paper proposed a Quick response code (QR code) based strategy to provide authentication to our digital images. Quick response code is used to provide protection to digital images because of its important characteristics like detection from 360° direction and large data encoding capacity. First of all, Least Significant Bit (LSB) approach is applied on the original image to select LSBs from each block of the image. Next, LSB image is partitioned into 8×8 sized blocks and mean is calculated for each block of the cell. Then Singular Value Decomposition function is performed on this cell to get singular values which are used as authentication data. After that QR Code generator is used to generate QR code matrix from these singular values. And finally this code is inserted into MSBs to get an authenticated image. Experimental result shows that proposed method produces images with good quality.

Index Terms*: *Image authentication, Least Significant bit, QR code, Singular Value Decomposition.

I. INTRODUCTION

The swift growth of digital technology uplifts its users to use this technology to communicate with each other (Wu & W. C. 2015). When digital data is transferred electronically from one user to another, this data can be forged by the illegal users, therefore by using image authentication method user can investigate whether images are attacked by attacker in between the channel or not. If yes, then altered areas are recognized and recuperated by using these authentication schemes. Image authentication approaches can be categorized as active and passive authentication which are used to provide authentication to digital content (Wu et al. 2016). There are two domains to insert authentication data into any image, spatial domain and frequency domain. Spatial domain based approaches are "Least Significant Bit (LSB)", "Local Binary Pattern (LBP)", and "Histogram modification" etc. In these methods the authentication data is inserted into the pixels of the original image.

Frequency domain based approaches are "Discrete Wavelet Transform (DWT)", "Discrete Cosine Transform (DCT)", and "Discrete Fourier Transform (DFT)" etc. In frequency domain based methods the authentication data is inserted into the coefficients of the original image (Qasim et al. 2018). The experimental result shows that quality of the authenticated image is good and this scheme can also locate the forged areas but the limitation of this scheme is that it is not able to recover the forged areas very efficiently. (Ansari et al. 2016) presented a singular value decomposition (SVD) based scheme to locate and recover the altered areas. The experimental result shows that the proposed scheme performs good in tamper detection but the recovery rate is satisfactory. (Wu & W. C. et al. 2016) introduces a SVD based scheme along with quick response code. This method produces the authenticated image with good quality and it performs well in recovering the altered areas. (Wu & Lin 2016) introduced two image authentication schemes. The author used SVD method along with the features of quick response code. SVD is used to compute the singular values which are used to produce authenticated data to generate quick response code. The proposed scheme performs good in generating and recovering authenticated image. But there is the problem of altered area detection. The limitation of this technique is that it is not capable of locating all the altered regions efficiently. (Ozyurt et al. 2018) introduced a hash function based colored image authentication method. The proposed strategy for colored images performs better in image authentication capability than previous method (Wu & Lin 2016). (Liu et al. 2018) applied a blind watermarking strategy where two watermarks are inserted into the primary image to provide it more security. Fragile watermark is inserted to perform authentication to images and imperceptible robust watermark used to provide copyright protection. (Dadkhah et al. 2014) introduced a "SVD" based approach to recognize and reconstruct the modified regions. And this approach has good capability to recognize the modified regions efficiently and can reconstruct these areas with good quality. (Zhang et al. 2013) represents a self-implanting based approach to insert fragile watermark into the image to recognize and recreate the changed or modified areas in order to provide protection. And this technique has the capability to generate a watermarked image with good quality. A "discrete shearlet transform" based strategy is applied in (Zhuvikin 2017), where it is used to extricate properties of the image. This method represents good results even with "JPEG compression".

This paper is partitioned into four sections. The proposed method for image authentication is discussed in section (2). Section (3) compares the results of the proposed method with the existing method. The last section (4) includes the conclusion of the whole paper along with future scope.

Revised Manuscript Received on June 15, 2019.

Sandeep Kaur,. Computer Science and Engineering, Punjab Engineering College, Chandigarh, India.
Alka Jindal, Computer Science and Engineering, Punjab Engineering College, Chandigarh, India.

II. PROPOSED SCHEME

The proposed method uses LSB, SVD and QR Code to implement self-embedding image authentication scheme. The basics of these method is discussed as follows:

A. ***Least Significant Bit (LSB):*** Least Significant Bit is a scheme used for watermarking in spatial domain (Qasim et al. 2018). In the proposed scheme we are using LSB technique to create quick response code which is inserted in the most significant bits of the image.

B. ***Singular Value Decomposition (SVD):*** SVD is a scheme taken from linear algebra which is used to decompose a matrix. This technique decomposes a matrix into three matrices. For example if we have matrix P of size $n \times n$ and when SVD function is applied on this matrix it is decomposed into s (diagonal matrix), u, and v (orthogonal matrices). Diagonal matrix contains its values called singular values only on diagonals and values other than diagonal values are zeros. These singular values are used to generate authentication data (Singh & Kaur 2014).

$$P = U \cdot S \cdot V^T = \sum_{k=1}^{n} u_k \cdot s_k \cdot v_k^T$$

$$= [u_1, u_2, \dots, u_n] \times \begin{bmatrix} s_1 & 0 \cdots 0 \\ 0 & s_2 \cdots 0 \\ \vdots & \vdots \ddots \vdots \\ 0 & 0 \cdots s_n \end{bmatrix} \times [v_1, v_2, \dots, v_n]^T \quad (1)$$

C. ***Quick Response Code:*** Quick Response code is two dimensional matrices which is used to store information. In the proposed scheme QR code is used to store authentication data of the image (Wu & Lin 2016).

The proposed scheme uses these methods for grayscale image authentication purpose. The step by step procedure of this scheme is given bellow:

Authentication data Embedding Scheme:

i. Firstly, 2nd LSBs are selected from the original image.
ii. After selecting LSBs from each pixel of the image, it is divided into 8×8 Block size. Now there is a 32×32 size cell, which contains these 8×8 sized Blocks.
iii. Mean of each 8×8 Block is calculated and then this cell is converted into matrix of 32×32 size.
iv. Now SVD function is applied on this matrix to get singular values.
v. s_1 singular values of each blocks are joined together and then this value is used as authentication data.
vi. QR Code generator is used to generate QR code from this authentication data.
vii. Generated QR code is inserted into the previously extricated MSBs and 1st LSB.
viii. The resultant produced image is authenticated image. Fig.1 represents the step by step procedure of the proposed embedding scheme using quick response code.

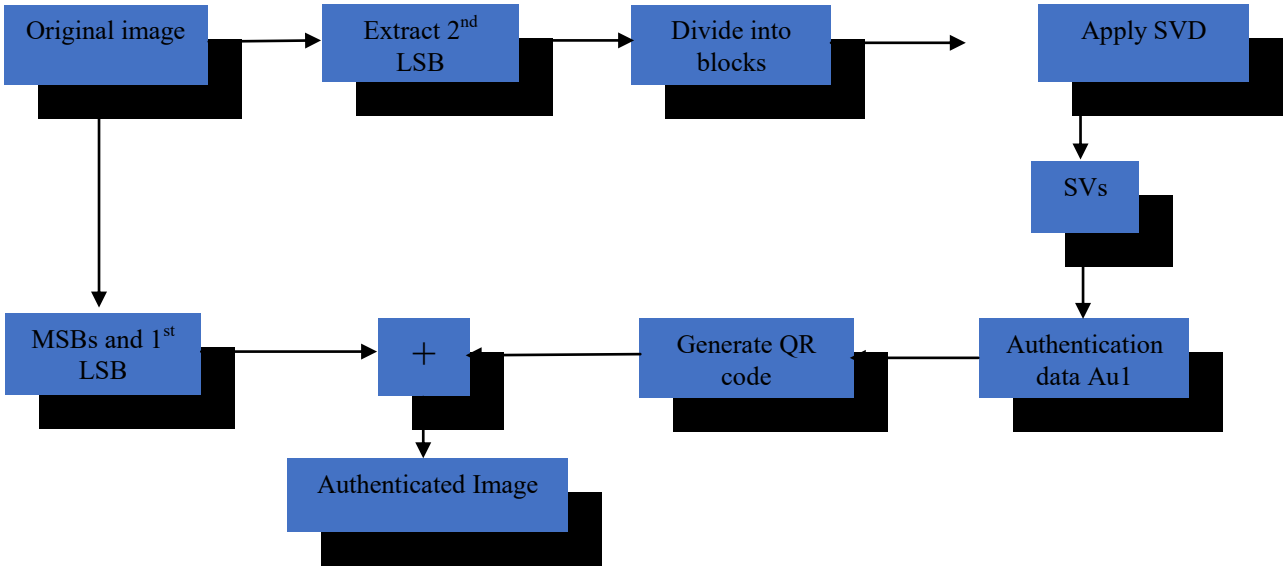


Figure 1: Block diagram of proposed data embedding scheme

Modification detection Scheme:

i. First of all, first LSBs are extricated from the authenticated image.
ii. Next, these bits are divided into 8×8 sized blocks.
iii. Then, SVD operation is applied on these blocks to get singular values from each of these blocks.
iv. After that, first singular values of each blocks are joined together.
v. Then, the value produced by joining all the first singular

values, is considered as first authentication data as (au1).

vi. On the other side, to calculate second authentication data (au2), six MSBs and 2nd LSB values are eliminated from the authenticated image in order to get embedded QR code.

vii. When this QR code is extricated from the authenticated image, then it is decoded to get second authentication data (au2).

viii. After that, both of these authentication data are compared.

ix. If both of compared authentication data (au1) and (au2) are same that means authenticated image is not modified or attacked.

x. On the other side if both of these authentication data do not match with each other means image is modified maliciously.

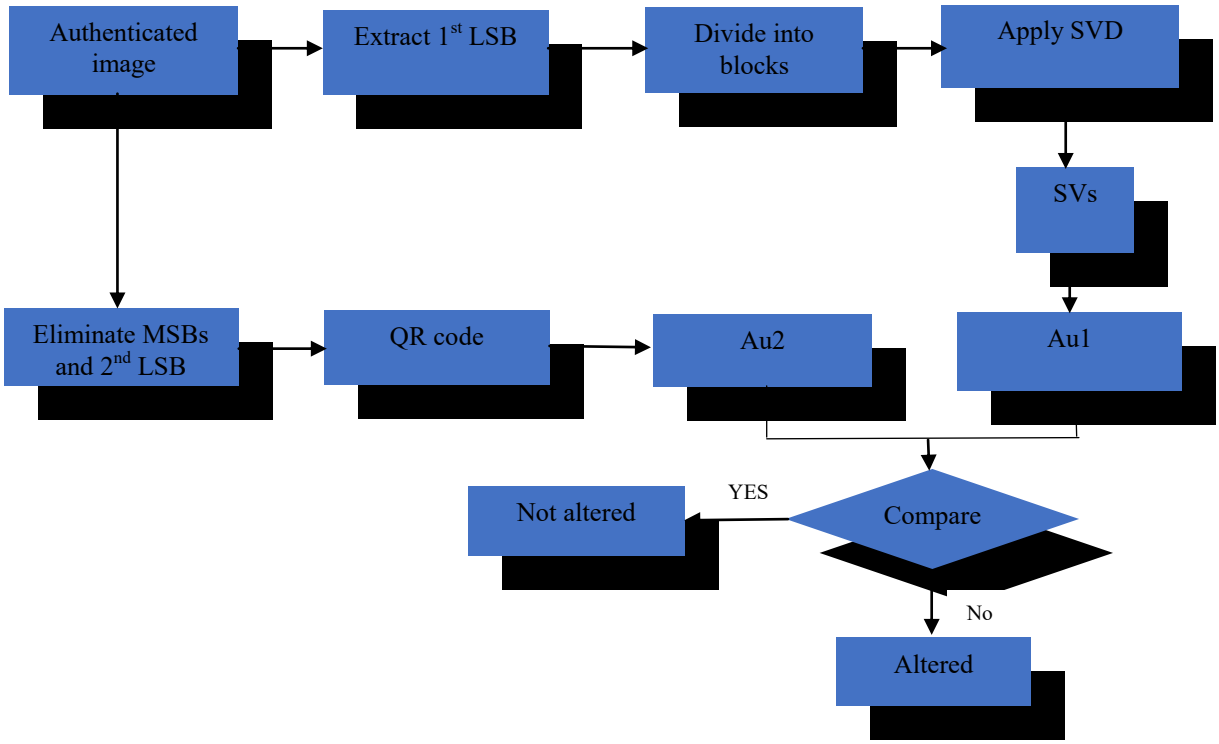


Figure 2: Tamper detection procedure

III. EXPERIMENTAL RESULTS

This method is executed on grayscale standard images of size 256×256 in MATLAB R2018a. In this method we have applied SVD function on 32×32 sized matrix. The generated 29×29 sized QR code matrix is first resized into 256×256 matrix then it is embedded into 256×256 matrix of MSBs to get an authenticated image. The quality of the implemented authentication scheme is tested using "Peak Signal to Noise Ratio (PSNR)". To calculate PSNR value of the authenticated image user need to calculate "Mean Squared Error (MSE)" value. These parameters are calculated using following equations:

A. Mean Squared Error (MSE) value: It is defined as the squared inaccuracy of the initial image with that of reconstructed image. It can be evaluated as follows (Qasim et al. 2018):

$$MSE = \frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} e(m,n)^2 \quad (2)$$

The term $e(m,n)$ is the inaccuracy between initial image and reconstructed image.

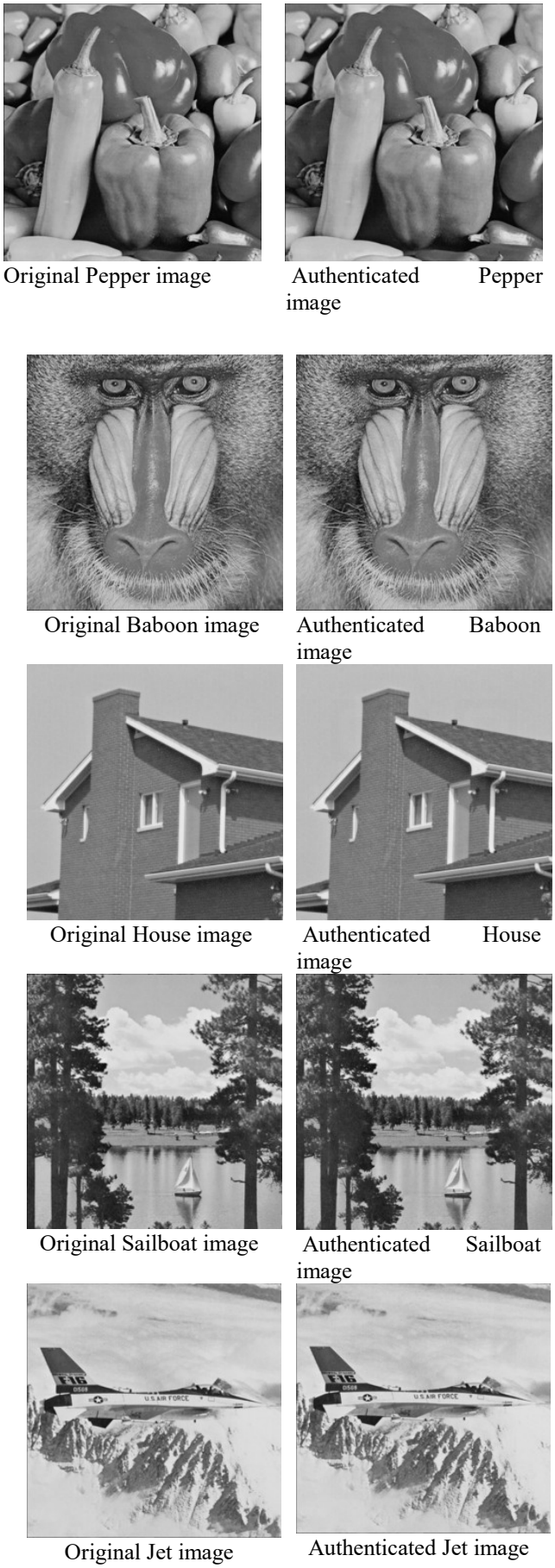
B. Peak Signal to Noise Ratio (PSNR): It is defined as the difference of the largest attainable range of a signal to that of the range of the noise that disturbs the authenticity of the image (Sreenivas & Kamkshi 2018):

$$PSNR = 10\log\frac{255^2}{MSE} \quad (3)$$

The results are shown in Table1 for different grayscale images. The observed outcomes indicate that the presented method is better for image authentication purpose and the results are given in the following table.

Table I: Comparison of proposed scheme with the existing scheme (Wu & Lin 2016)

Image	Wu et al. Scheme1	Wu et al. Scheme2	Proposed Scheme
Pepper	51.10	51.12	58.26
Baboon	51.10	51.15	58.16
House	51.15	51.16	57.51
Sailboat	51.16	51.14	57.85
Jet	51.12	51.13	58.18



Original Pepper image | Authenticated Pepper image

Original Baboon image | Authenticated Baboon image

Original House image | Authenticated House image

Original Sailboat image | Authenticated Sailboat image

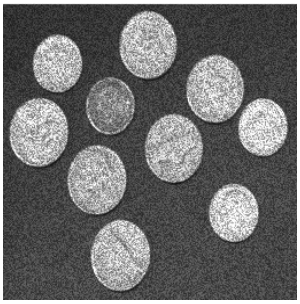
Original Jet image | Authenticated Jet image

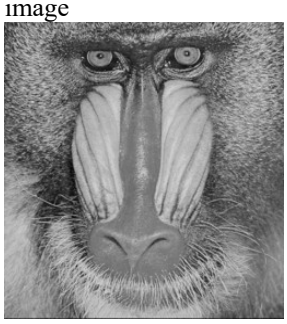
Figure 3: Original and authenticated images produced with proposed scheme

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig.3 displays the original images and their respective authenticated images. The experimental result shows that the proposed scheme produces images with better quality as compare to the scheme that was used in (Wu & Lin 2016). The average quality of the authenticated image is 57.99dB.
The alter detection procedure is used to observe whether authenticated image is altered maliciously or not. By utilizing this proposed scheme receiver can identify that image is same as sent from sender side by calculating two values au1 and au2. In order to check the alteration in the authenticated image two attacks are performed on the authenticated image. These attacks are applied by adding Speckle noise and Poisson noise into the authenticated image. Then both authentication data values of au1 and au2 are calculated for these attacked images. Fig.4 shows the produced authenticated images and images by applying speckle noise on these authenticated images.


Authenticated Coins image


Attacked Coins image


Authenticated Baboon image

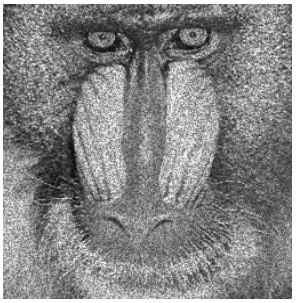
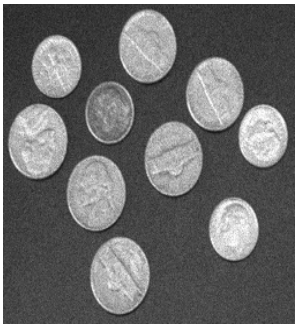
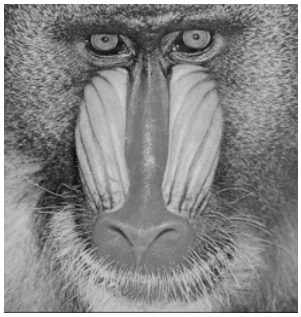

Attacked Baboon image

Figure 4: Authenticated images and their respective images with speckle noise


Authenticated Coins image


Attacked Coins image


Authenticated Baboon image

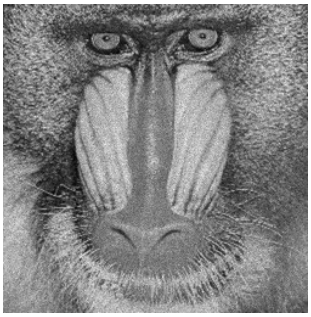

Attacked Baboon image

Figure 5: Authenticated images and their respective images with Poisson noise

The experimental observed result shows that the values of authentication data are almost same when produced from authenticated images. And these values are not same for attacked images. The results of authentication data values produced for authenticated image and attacked image are given below in the table.

Table II: Results of detected authentication data values

Authenticated image		
	Au1 (dB)	Au2 (dB)
Coins	0.0630	0.0978
Baboon	0.0627	0.0976
Images after adding Speckle noise		
Coins	NaN	0.0641
Baboon	NaN	0.0632
Images after adding Poisson noise		
Coins	NaN	0.0629
Baboon	NaN	0.0630

IV. CONCLUSION

The scheme presented in this paper uses singular values to generate authentication data. These singular values are joined together and converted into QR code using QR code generator. We have used quick response code for data embedding and extrication process because of its features like QR code can store large amount of data and because of its reliable readability to decode this code into original form. In this paper our scheme mainly focusses on generating the authenticated images with good quality. This method produces the authenticated images with average quality of 57.99dB. In alter detection process two values are extricated from the authenticated image which are compared to check the originality of the authenticated. Local binary pattern (LBP) is a spatial domain based scheme which can be utilized to authenticate images. There is a scope of getting authenticated image with good quality.

REFERENCES

1 Ansari, I. A., Pant, M., & Ahn, C. W. (2016). SVD based fragile watermarking schem e for tamper localization and self-recovery. *International Journal of Machine Learning and Cybernetics*, *7*(6), 1225–1239. https://doi.org/10.1007/s13042-015-0455-1

2 Dadkhah, S., Abd Manaf, A., Hori, Y., Ella Hassanien, A., & Sadeghi, S. (2014). An effective SVD-based image tampering detection and self-recovery using active watermarking. *Signal Processing: Image Communication*, *29*(10), 1197–1210. https://doi.org/10.1016/j.image.2014.09.001

3 Liu, X. L., Lin, C. C., & Yuan, S. M. (2018). Blind Dual Watermarking for Color Images' Authentication and Copyright Protection. *IEEE Transactions on Circuits and Systems for Video Technology*, *28*(5), 1047–1055. https://doi.org/10.1109/TCSVT.2016.2633878

4 Ozyurt, F., Tuncer, T., & Avci, E. (2018). A novel probabilistic image authentication method based on universal hash function for RGB images. *2018 International Conference on Computing Sciences and Engineering, ICCSE 2018 - Proceedings*, 1–6. https://doi.org/10.1109/ICCSE1.2018.8373994

5 Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, *27*, 45–60. https://doi.org/10.1016/j.cosrev.2017.11.003

6 Singh, H., & Kaur, L. (2014). Fractional M-band dual tree complex wavelet transform for digital watermarking, *39*(April), 345–361.

7 Sreenivas, K., & Kamkshi Prasad, V. (2018). Fragile watermarking schemes for image authentication: a survey. *International Journal of Machine Learning and Cybernetics*, *9*(7), 1193–1218. https://doi.org/10.1007/s13042-017-0641-4

8 Wu, W. C. (2015). Subsampling-based image tamper detection and recovery using quick response code. *International Journal of Security and Its Applications*, *9*(7), 201–216. https://doi.org/10.14257/ijsia.2015.9.7.18

9 Wu, W. C., Chan, C. S., Lin, C. Y., & Lin, Z. W. (2016). Joint SVD and QR codes for image authentication. *2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2015*, (December), 1137–1140. https://doi.org/10.1109/APSIPA.2015.7415448

10 Wu, W., & Lin, Z. (2016). SVD-Based Self-Embedding Image Authentication Scheme Using Quick Response Code Features. *JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION*, (February). https://doi.org/10.1016/j.jvcir.2016.02.005

11 Zhang, J., Zhang, Q., & Lv, H. (2013). Optik A novel image tamper localization and recovery algorithm based on watermarking technology. *Optik - International Journal for Light and Electron Optics*, *124*(23), 6367–6371. https://doi.org/10.1016/j.ijleo.2013.05.040

12 Zhuvikin, A. (2017). Selective Image Authentication Using Shearlet Coefficients Tolerant to JPEG Compression. *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems*, *11*, 681–688. https://doi.org/10.15439/2017f177

AUTHORS PROFILE

Sandeep Kaur, currently pursuing M.Tech in Computer Science and Engineering (Information Security) from Punjab Engineering College Chandigarh. Her area of interest includes Image Processing and Biometric Security.

Alka Jindal, Assistant Professor in department of Computer Science and Engineering in Punjab Engineering College Chandigarh. Her area of interest includes image processing, Security, and Database Systems. e-mail : alka_er@rediffmail.com