Digital Signature Protocol for Visual Authentication

Anirban Goswami[1], Ritesh Mukherjee[2], Soumit Chowdhury[3], and Nabin Ghoshal[4]
[1]Department of Information Technology, Techno India, India
[2]Department of Advanced Signal Processing, Centre for Development of Advanced Computing, India
[3]Department of Computer Science and Engineering, Government College of Engineering and Ceramic Technology, India
[4]Department of Engineering and Technological Studies, University of Kalyani, India

Abstract: *Information security in digital domain is all about assurance of Confidentiality, Integrity, Availability (CIA) extending authenticity and non-repudiation issues. Major concerns towards implementation of information security are computational overhead, implementation complexity and robustness of the protocol. In this paper, we proposed a solution to achieve the target in line with state of the art information security protocol. The computational overhead is significantly reduced without compromising the uncertainty in key pair generation like existing digital signature schemes. The first section deals with collection of digitized signature from an authentic user, generation of shares from the signature, conversion of a cover image to quantized frequency form and casting of a share in appropriate coefficients. In the second section, share detection is done effectively and the data security is confirmed by overlapping the detected share with the other share. Specific constraints are fitted appropriately to recreate a clean digitized signature, reform the cover image using Discrete Cosine Transform (DCT) and quantization method, select frequency coefficients for share casting and manipulate the casting intensity. Impressive effort is made to ensure resistance to some of the common image processing attacks. The undesired white noise is reduced considerably by choosing a suitable threshold value. The selection of pseudorandom hiding position also helps to increase the robustness and the experimental results supports the efficacy of the algorithm.*

Keywords: *Share, DCT and IDCT, image compression, data hiding, SSIM, collusion attack.*

Received July 6, 2016; accepted August 21, 2017

1. Introduction

The technological escalation and elaborate use of the network domain has extended the use of the Internet. But this advancement has proportionally increased the importance to shield confidential or copyright information through efficient techniques. The most common method of information confidentiality is to encrypt and then imperceptibly hide the sensitive data to restrain intruders.

Some of the existing data hiding techniques explained fabrication of authentication signals into a digital file for assuring the integrity or fidelity of the file [15, 19, 24]. The application of copyright protection also depicts content ownership claim where a digital file is used to embed a visible or invisible digital watermark [2]. In case of covert communication [11, 14] secret information is hidden into a cover file and the intended receiver only can extract the hidden information to complete the communication.

The generation of shares from an information and subsequent sharing of the shares was first explained by Shamir [20]. The challenge is in recovering the information appropriately when the related shares are combined. Conventionally, the two concepts viz. data hiding and information sharing can both be an integral part of information security.

Nowadays researchers are concentrating more on encryption and masking based image authentication techniques [7, 12] along with exploiting the redundant information of an image to fabricate the secret information. In context to the authentication method, the existing algorithms can be broadly classified as spatial and transform domain techniques. In the spatial domain techniques, high volume of payload can be fabricated with minimum computational complexity but less resistance to low pass filtering and common image processing attacks. Hence widely accepted algorithms are mostly in transform domains i.e., Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) etc., [16, 21, 22]. Prior to these transform techniques, the concept of Spread Spectrum based watermarking techniques also exploited Human Visual Systems (HVS) [5, 9, 18].

Cox *et al*. [5] suggested DCT domain to be an extensively used transform in Joint Photographic Experts Group (JPEG) compression. In DCT domain the possibility of coefficients getting affected by compression are known at prior and as a protective measure use of middle-band frequency coefficients to embed the secret data was first proposed by Koch and Zhao [9].

As per the study of the existing research, some spatial and transform domain techniques are chronologically mentioned. Bender *et al*. [3] suggested embedding of a secret message in the least significant bits of image pixel values. A modified technique was proposed by Nikolaidis and Pitas [17] where the numbers of bits were fabricated as in the conventional method but in adaptive manner. But due to the ease in deciphering the secret data in spatial domain by an intruder, the focus was shifted to transform domain. Barni *et al*. [1] proposed a technique where the image blocks were transformed into frequency coefficients by applying DCT and secret bits were embedded in the frequency components. In another algorithm, Sara Tedmori and Al-Najdawi [23] mentioned an encryption based fabrication in high and low frequency regions of a DCT based algorithm.

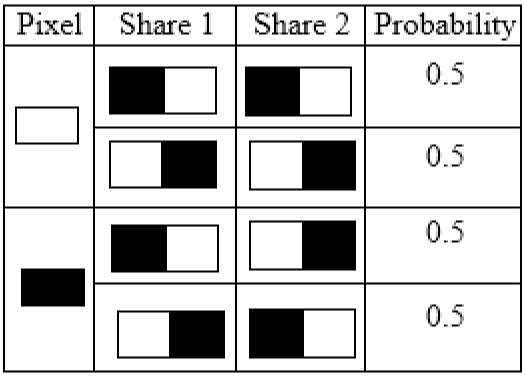
But due to the disturbance caused by image compression attack, a concept of utilizing the middle frequency coefficients for embedding was proposed by Hsu and Wu [8]. In an algorithm, Langelaar *et al*. [10] confirmed that if the middle frequency bands are chosen for embedding, the watermark information don't get scattered to most visual important parts i.e., low frequency areas of the image. Lin *et al*. [13] also utilized the mid frequency band for embedding to resist JPEG compression attack. Hence it can be inferred that the utility of middle frequency band in DCT domain [4] provides a resistance and keep the casted secret data undisturbed if compression and noise attacks are applied.

The proposed algorithm have considered the positive aspects of using the mid band area of the DCT domain. The concept of neural network based approach for visual cryptography is incorporated to justify the issues of data security viz. Confidentiality, Integrity, Authentication and Non-repudiation, along with the proposed imperceptible data hiding mechanism. The next section describes the overall research methodology.

2. The Research Method

The proposed algorithm has been divided into three phases. The first two phases are performed at the sender's end and the last phase is performed at the receiver's end. The phases are defined as:

- *Phase* 1: A Digitized Signature (DS) is considered a utility function for public-key (asymmetric) cryptography scheme and facilitates entity authentication, data integrity and non-repudiation [6]. In the proposed algorithm we have collected a digitized signature and a self-derived threshold based cleaning mechanism is used to convert the signature into a stream of black and white pixels only. The black and white pixels are made distinct such that even after some image processing operations are applied, significant amount of black pixels can be detected to reconstruct the signature. Two distinct shares are generated from each of the black or white pixel values as mentioned in neural network based approach for visual cryptography by Yue and Chiag [25].



Pixel	Share 1	Share 2	Probability
□	■□	■□	0.5
	□■	□■	0.5
■	■□	□■	0.5
	□■	■□	0.5

Figure 1. Technique for generation of shares.

The Share 1 (S1) and Share 2 (S2) are treated as the private and public shares of the sender respectively. S1 is casted in a cover image and S2 is made available to the receiver. The key issues of data security are handled properly as:

1. At the receiver's end, if S2 can be fed to the detection algorithm and which when combined with S1 generates a valid signature, the authenticity of the sender and the sent document can both be validated.
2. If the communicated document contains S1 (private share), the receiver contains S2 (public share) and the combination (S1+S2) forms a valid signature then non-repudiation property holds. The sender cannot deny the fact that the document containing S1 not being communicated from his end because S1 is a private share and only known to the sender.
3. S1 cannot be extracted (private) but can only be combined with S2 internally through detection algorithm to generate a signature. This states the property of confidentiality.
4. If a secret document is to be safely preserved then a public share of an individual is casted properly and the private share of the respective individual is only used to authenticate the document.

- *Phase* 2: In the standard image compression i.e. JPEG transformation, the concept is based on the energy minimization after DCT. This causes loss of information in high frequency domain in case of lossy compression. The proposed algorithm has been designed to prevent information loss even after JPEG compression is affected. Firstly, the cover image partitioned as non-overlapping 8x8 blocks is levelled off and transformed to frequency domain on application of two dimensional DCT. Due to effective image compression and decent image quality after decompression a quality level 50 is considered which is represented as Q_{50} quantization matrix. A technique of rounding the fractional value is also done to further support prevention of data loss. A self-defined operation is executed to generate pseudorandom hiding position in the middle frequency band of every alternate block. The reason for implementing the hiding technique after the execution of the steps: Levelling, DCT, Quantize and round off, is to avoid any data loss further that may occur due to the effect of JPEG compression attack on the modified image. Moreover, due to choice of alternate blocks and pseudorandom hiding positions the collusion attack can also be resisted.

- *Phase* 3: The detection algorithm is executed at the receiver's end to detect S1 and combined with S2 to obtain the valid signature, which proves the authenticity of the receiver. Moreover, exact detection of S1 supports the integrity property of data security and also the authenticity of the sender.

Section 3 describes the algorithm in detail.

3. Discussion of the Algorithm

The stages are:

- Cleaning of the Payload Data: A digitized signature is considered as a payload and the mechanism is defined as:

$$P(x, y) < T \ ?\ CP(x, y) = 0 : CP(x, y) = 255 \qquad (1)$$

$P(x, y)$ is the intensity value at (x, y) position of the payload data. T is a threshold value which is defined depending on the intensity variance of all the pixel values of the payload. $CP(x, y)$ is the modified intensity values at the same position of the reconstructed payload format. The values of $CP(x, y)$ refer to only black and white intensity values. A stream of black and white values is generated.

- Generation of Shares

The format of two shares (S1 and S2) depends on the intensity value defined by CP(x, y). The mathematical formula to generate the shares is:

(CP(i,j)==0) ? S1(i,2*j-1)=255,S1(i,2*j)=0, S2 (i, 2*j-1) = S1 (i, 2*j), S2(i, 2*j) = S1(i, 2*j-1) : (mod (random ([m n]), 2) == 0) ? S1(i, 2*j-1) = 255, S1(i,2*j) = 0, S2(i, 2*j-1) = S1(i,2*j-1), S2(i, 2*j) = S1(i,2*j) : S1(i,2*i-1)= 0; S1(i,2*j) = 255, S2(i, 2*j-1) = S1(i,2*j-1),S2(i,2*j)=S1(i,2*j); (2)

Where i varies from 1 to r, j varies from 1 to c and r, c are the width and height of the payload data. The values of m and n are taken arbitrarily. Pictorially it is represented as:

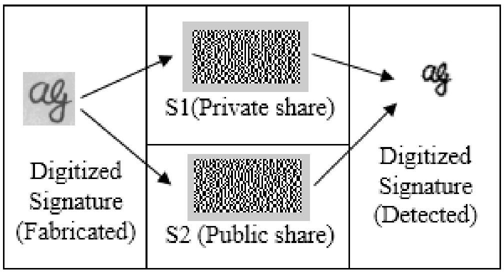


Figure 2. Representation of the digitized signature.

- Generation of pseudorandom positions: The pseudorandom position denoted as ipos is initially taken as 0. The selection of a block (k) is determined by mod(k, 2). The value of ipos is mathematical derived as:

$$\begin{aligned}
&\mathit{Binary}\ (ipos) = (I_n),\ n \text{ varies from 1 to 8.}\\
&m = I_8I_7I_6I_5.\\
&d_1 = (I_8I_7)\ XOR\ (I_6I_5) = d_{11}d_{12}.\\
&\mathit{Binary}\ (k) = (K_n),\ n \text{ varies from 1 to 8.}\\
&e = K_8K_7K_6K_5.\\
&d_2 = (K_8K_7)\ XOR\ (K_6K_5) = d_{21}d_{22}.\\
&d_3 = d_1\ XOR\ d_2 = d_{31}d_{32}.\\
&ipos = Dec\ (d_3) = \text{any value from 0 to 3.}\\
&ipos = (ipos == 0\ ||\ ipos == 1)\ ?\ 1 : (ipos == 2)?\ 2:3.
\end{aligned} \qquad (3)$$

- Payload Hiding Process

Input: A gray Image as cover and a share as the payload.
Output: An authenticated Image.
The cover image is considered as a set of non-overlapping 8x8 pixel blocks. Steps 1 to 5 are repeated for each of the selected blocks till the payload gets fully casted.

- *Step* 1: Basically, DCT is effective on the pixels with intensity values ranging from -127 to 128. So the intensity values of the current block are levelled off by subtracting 128 from all values individually.
- *Step* 2: The signed integer values [–127 128] are converted to frequency coefficients by applying forward DCT formula (Equation 4) on the current block.

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \qquad (4)$$

Where $0 \leq p \leq M-1$ and $0 \leq q \leq N-1$.
The terms a_p and a_q are represented as,

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \frac{\sqrt{2}}{M}, & 1 \leq p \leq M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \frac{\sqrt{2}}{N}, & 1 \leq q \leq M-1 \end{cases}$$

The values B_{pq} are called the DCT coefficients of spatial value A_{mn}.

- *Step* 3: The frequency coefficients are quantized by using Q_{50} and rounded off to the nearest integer. This is done to distribute the energy of the image amongst low, medium and high frequency zone. Any modification in the low frequency zone generally produces visual alterations in the cover image, whereas the high frequency zone is shredded off by JPEG quantizer. Only the coefficients that are resistant to JPEG algorithm are used for share casting by performing parametric modifications on the selected coefficients.
- *Step* 4: Selection of the appropriate coefficient in the middle frequency zone is done pseudo-randomly and the process is implemented as:

(flag == true) ? (S1(w) == 0) && (ipos == i) ?

CI(i, 7-i) < 0 ? diff = 0 - CI(i, 7-i), CI(i, 7-i) = CI(i, 7-i) + (diff + d) : (CI(i, 7-i) == 0) ? CI(i, 7-i) = CI(i, 7-i) + d : CI(i, 7-i) = CI(i, 7-i) : (S1(w) == 255) && (ipos == i) ? CI(i, 7-i) > 0 ? diff = CI(i, 7-i) – 0, CI(i, 7-i) = CI(i, 7-i) - (diff + d) : (CI(i, 7-i) == 0) ? CI(i, 7-i) = CI(i, 7-i) - d : CI(i, 7-i) = CI(i, 7-i) : (5)

Index values of *CI* are swapped for both black and white intensity values of *S1*(*w*).

The flag variable is used to alternate the index values of *CI* for the same value of ipos. *S*1(w) is the payload vector denoting the intensity value at position w. The value of *i* is determined by ipos. *CI*(*i*, 7-*i*) denotes the intensity value of the cover image pixel at location (*i*, 7-*i*). The value of the variable d is determined effectively so as to maintain an acceptable distortion level of the image after hiding i.e., imperceptible to HVS.

- *Step* 5: Reconstruction is done by multiplying each element of the current block with the corresponding element of Q_{50}.
- *Step* 6: Inverse DCT (IDCT) (Equation 6) is applied on the current block and the generated values are rounded to the nearest integer. The decompression procedure is completed by adding 128 to each of the values. The generated 8x8 block is written to its designated location in the output image in row major order.

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \qquad (6)$$

Where $0 \leq m \leq M-1$ and $0 \leq n \leq N-1$.

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \frac{\sqrt{2}}{M}, & 1 \leq p \leq M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \frac{\sqrt{2}}{N}, & 1 \leq q \leq M-1 \end{cases}$$

- Payload Detection Process

Input: An authenticated image.

Output: Signature.

The input image is considered as a set of non-overlapping 8x8 pixel blocks. Steps 1 to 4 are repeated for each of the selected blocks until the payload gets fully detected.

Step 1: The intensity values of the current block are levelled off by subtracting 128 individually from all values.

Step 2: The signed integer values [–127 128] are converted to frequency coefficients by applying forward DCT formula (Equation 4) for 8 x 8 block.

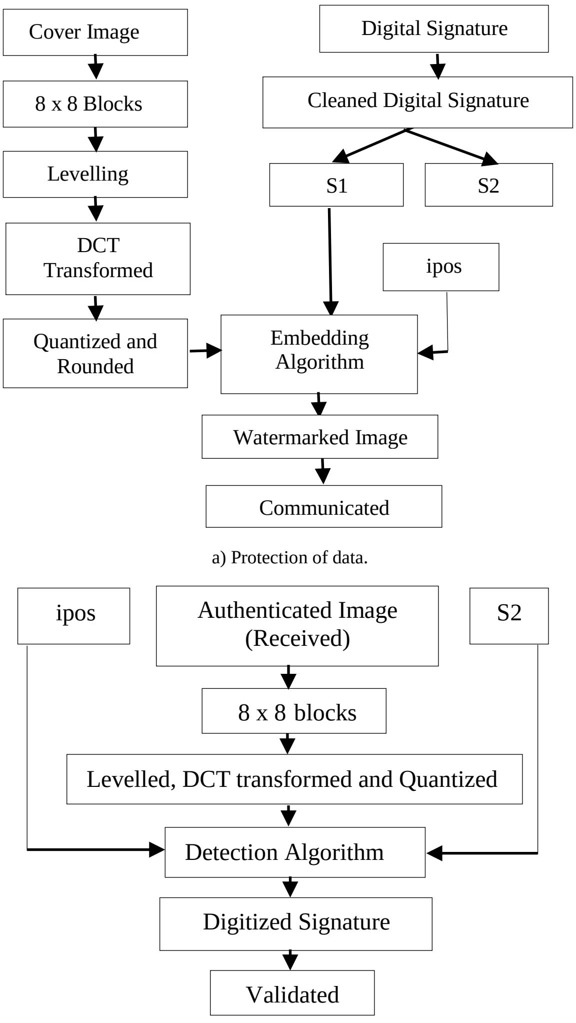
Step 3: The frequency coefficients are quantized by using Q_{50}.

Step 4: The detection technique is implemented as:

(flag == True) ? (ipos == i) ? (WI (i, 7-i) > 0)? S1E (w) = 0: S1E (w) = 255.
(flag==false)?(ipos == i)?(WI (7-i, i) > 0)? S1E (w)= 0: S1E(w)=255. (7)

The meaning of the flag variable is similar to that used in the payload hiding algorithm. *WI* is the authenticated image and S1E is the share vector. When all the values are properly detected, S1E is converted to 2D format to form the share *S11*. The public share *S2* is combined with *S11* to form the valid signature at the receiver's end.

The flowchart of the algorithmic steps is shown in Figure 3.



a) Protection of data.

b) Validation of data.

Figure 3. Flow chart of the algorithm.

4. Performance Analysis

- Result Simulation using Metrics: A number of gray scale images are used in experimenting with the proposed algorithm. This section describes:

1. The effect of the proposed algorithm when tested on the cover images eg. airplane, baboon, boat, chilli, fruits, goldhill, kaya etc.
2. The effect of choosing different intensity values related to fabrication.

3. The performance of the algorithm in terms of the image quality metrics namely, MSE, PSNR, SSIM, IF and Correlation Coefficient.

Some of the images taken as input are shown in Figure 4 (a, c, e, and g) respectively and the authenticated images are shown in Figure 4 (b, d, f, and h) respectively. Comparing the images pairwise, it can be stated that the cover images are visually identical to the modified images, although the mid frequency band holds the message data.

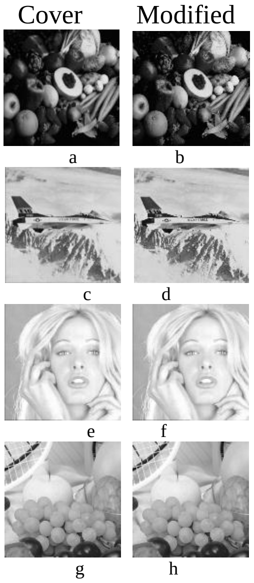
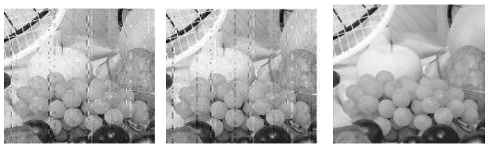


Figure 4. Visual interpretation.

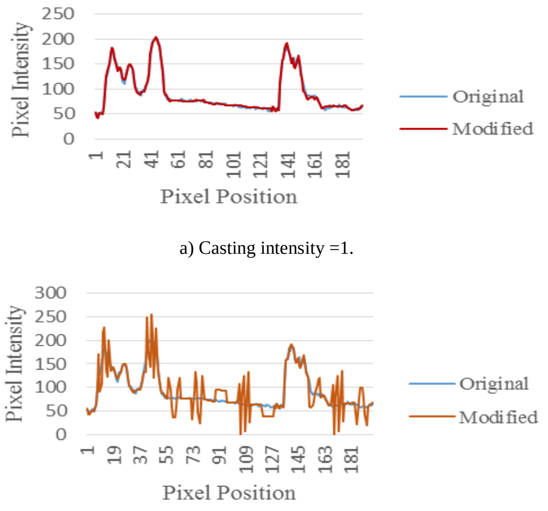
Further experimenting with different intensity values of t that is used in the hiding formula W = tC (W and C are the authenticated and cover images respectively) and the effect on the authenticated images are shown in Figure 5. The value of t helps to control the degree of white noise in the authenticated image and in turn increases the imperceptibility of the image even after modification. The variance is shown graphically in Figure 6.



T=2. T=4. T=1.

Figure 5. Images with different casting intensity.

In Figures 6-a and 6-b, the best case is considered at intensity value = 1. In rest of the values of intensity determined by the different values of i as considered in the experimentation, the graphical difference between the original and authenticated images is very much distinct.



a) Casting intensity =1.

b) Casting intensity = 2i.

Figure 6. Graphical Comparison at different casting intensities.

In the last part, after experimentation the subsequent results related to the image quality metrics viz. MSE, PSNR, IF, SSIM and CC are shown in Table 1.

Table 1. Performance analysis.

Images	MSE	PSNR	IF	SSIM	CC
Chilli	4.2590	42.3605	0.9664	0.9980	0.9979
Fruits	6.5246	40.1253	0.9570	0.9984	0.9983
Kaya	6.2211	40.3545	0.9671	0.9986	0.9989
Lenna	8.2781	39.2419	0.9287	0.9963	0.9964
Peppers	9.0025	39.0127	0.9158	0.9931	0.9950
Tiffany	9.8812	38.9123	0.9012	0.9812	0.9914
Vegetables	8.0234	39.8712	0.9341	0.9982	0.9971
Watch	10.8910	37.7889	0.8298	0.9933	0.9926
Grapes	9.3263	39.4337	0.9395	0.9965	0.9962
Airplane	8.3243	40.1234	0.9331	0.9968	0.9981
Average	**8.07315**	**39.72244**	**0.92727**	**0.99504**	**0.99619**

The values of the different metrics in the above table suggest that the fabricated secret data is quite imperceptible to human eyes.

- *Effectiveness Against other Techniques*: The proposed technique is also compared with some of the existing techniques in terms of PSNR as shown in Figure 7.

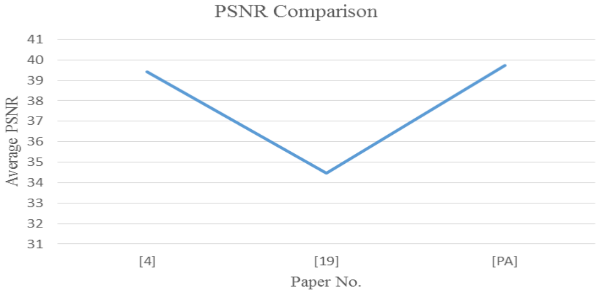


Figure 7. Comparison of PSNR value.

- *Resistance to attacks*: The proposed algorithm has been tested at different compression quality and the secret data can be detected reasonably successfully to reform the digitized signature. The testing results shown in Figure 8 signify losslessness supportive algorithm.

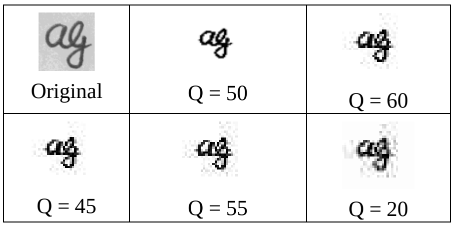


Figure 8. Framed payload from different quality compression of the chilli image.

To resist collusion attack, the hiding position is made pseudorandom. So, the attacker may not be able to study different authenticated images and ascertain the pattern and casting position.

Moreover due to pseudo-variant casting location, the attacker may not be able to predict the hiding location and hidden data by combining many copies of the authenticated image. In other words, the Averaging technique, i.e., $g(x, y) = f(x, y) + n(x, y)$, where $g(x, y)$ is the generated noisy image formed by addition of noise $n(x, y)$ to an image $f(x, y)$, will not be very effective. In averaging with similar authenticated images, $g(x, y)$ will not be similar to $f(x, y)$ as $n(x, y)$ never reaches zero value.

For effectiveness of the visual attack the issues:

1. Sequential fabrication of the secret data.
2. Bit plane size must be greater than the payload size.
3. The binary format of the secret data is required instead of encryption. In the proposed algorithm all the three issues are restricted to avoid the attack.

An effort is also made to eliminate the white noise by controlling the casting intensity.

- *Complexity analysis*: The time complexity of the proposed algorithm is calculated considering the size of the share and an integer G whose value is taken as >=2, representing a secret information in form of two shares (non-expendable format of visual cryptography).

If the size of each of the shares are n x n respectively then the time complexity to generate the two shares (S1, S2) are each $O(n^2G)$ respectively. So the total time complexity for generation of the two shares is $O(n^2G)$. In the reconstruction phase, the time complexity required to combine the two shares and recover the original signature is $O(n^2G)$ also. In addition to this, the time expended in taking the signature at the sender's and the receiver's end and verifying the signature at the receiver's end are also included in determining the time complexity of the algorithm.

5. Conclusions

The thought of supporting and strengthening the four important aspects of data security has indulged in developing the proposed algorithm. An amalgamation of visual cryptography and imperceptible data hiding has been done to support the fact. The algorithm has been designed effectively which may improve losslessness with increased robustness and low visual artifacts. The detection of watermark can be properly done at the receiver's end without the need of the original image. Hence, the proposed technique may be extensively used for copyright protection and secure military documents during storage and necessary communication.

References

[1] Barni M., Bartolini F., Cappellini V., and Piva A., "A DCT Domain System For Robust Image Watermarking," *Signal Processing*, vol. 66, no. 3, pp. 357-372, 1998.

[2] Barni M., Bartolini F., and Furon T., "A General Framework For Robust Watermarking Security," *Signal Processing*, vol. 83, no. 10, pp. 2069-2084, 2003.

[3] Bender W., Gruhl D., Morimoto N., and Lu A., "Techniques for Data Hiding," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 313-336, 1996.

[4] Chaturvedi R., Sharma A., Hemrajani N., and Goyal D., "Analysis of Robust Watermarking Technique Using Mid Band DCT Domain for Different Image Formats," *International Journal of Scientific and Research Publications*, vol. 2, no. 3, pp. 1-4, 2012.

[5] Cox I., Kilian J., Leighton T., and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[6] Diffie W. and Hellman M., "New Directions in Cryptography," *IEEE Transactions in Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[7] Gao X., An L., Li X., Tao D., Deng C., and Li J., "Robust Reversible Watermarking Via Clustering and Enhanced Pixel-Wise Masking," *IEEE Transactions on Image Processing*, vol. 21, no. 8, pp. 3598-3611, 2012.

[8] Hsu C. and Wu J., "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing*, vol. 8, no. 1, pp. 58-68, 1999.

[9] Koch E. and Zhao J., "Towards Robust and Hidden Image Copyright Labelling," *in Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, pp. 452-455, 1995.

[10] Langelaar G., Setyawan I., and Lagendijk R., "Watermarking Digital Image and Video Data,"

IEEE Signal Processing Magazine, vol. 17, no. 5, pp. 20-46, 2000.

[11] Lee I. and Tsai W., “A New Approach to Covert Communication Via PDF Files,” *Signal Processing*, vol. 90, no. 2, pp. 557-565, 2009.

[12] Lee C. and Tsai W., “A Secret-Sharing-Based Method for Authentication of Grayscale Document Images Via the Use of the PNG Image with A Data Repair Capability,” *IEEE Transactions on Image Processing*, vol. 21, no. 1, pp. 207-218, 2012.

[13] Lin S., Shie S., and Guo J., “Improving the Robustness of DCT Based Image Watermarking Against JPEG Compression,” *Computer Standards and Interfaces*, vol. 32, no. 1-2, pp. 54-60, 2010.

[14] Liu T. and Tsai W., “A New Steganographic Method for Data Hiding in Microsoft Word Documents by A Change Tracking Technique,” *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 24-30, 2007.

[15] Lu C. and Liao H., “Multipurpose Watermarking for Image Authentication and Protection,” *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579-1592, 2001.

[16] Meerwald P. and Uhl A., “A Survey of Wavelet-Domain Watermarking Algorithm,” *in Proceedings of Electronic Imaging, Security and Watermarking of Multimedia Contents III*, San Jose, pp. 505-515, 2001.

[17] Nikolaidis N. and Pitas I., “Robust Image Watermarking in the Spatial Domain,” *Signal Processing*, vol. 66, no. 3, pp. 385-403, 1998.

[18] Ruanaidh J. and Pun T., “Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking,” *Signal Process*, vol. 66, no. 3, pp. 303-317, 1998.

[19] Saini M., Venkata K., and Kalra G., “Comparative Analysis of Digital Image Watermarking Techniques in Frequency Domain using MATLAB SIMULINK,” *International Journal of Engineering Research and Applications*, vol. 2, no. 4, pp. 1136-1141, 2012.

[20] Shamir A., “How to Share A Secret,” *Communication of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[21] Solachidis V. and Pitas I., “Circularly Symmetric Watermark Embedding in 2-D DFT Domain,” *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753, 2001.

[22] Suhail Mohamed A. and Obaidat S., “Digital Watermarking-Based DCT and JPEG Model,” *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640-1647, 2003.

[23] Tedmori S. and Al-Najdawi N., “Lossless Image Cryptography Algorithm based on Discrete Cosine Transform,” *The International Arab Journal of Information Technology*, vol. 9, no. 5, pp. 471-477, 2012.

[24] Yu G., Lu C., and Liao H., “Mean Quantization-Based Fragile Water-Marking for Image Authentication,” *Optical Engineering*, vol. 40, no. 7, pp. 1396-1408, 2001.

[25] Yue T. and Chiag S., “A Neural Network Approach for Visual Cryptography,” *IEEE-INNS-ENNS International Joint Conference on Neural Networks*, Como, pp. 494-499, 2000.

Anirban Goswami is currently working as Asst. Professor and Asst. Registrar in Techno India (An Engineering College under Maulana Abul Kalam Azad University of Technology), Kolkata, West Bengal, India. He has more than 17 years of teaching experience He had contributed in more than 6 graduate level projects, and has 9 international conference and 5 international journal publications. He is currently pursuing his research work on data security in Kalyani University.

Ritesh Mukherjee is associated with C-DAC (Centre for Development of Advanced Computing), Kolkata, India as Joint Director. He has 17 years of experience in software solution development in the area of large database, data warehousing, Web technologies, Mobile Computing etc. He had contributed in more than 12 projects, release of 6 solutions and 2 products. He has 4 research papers in various journals and conferences, 3 copyrights, 1 Indian and 1 US patents.

Soumit Chowdhury is presently working in the position of Assistant Professor of the dept. of Computer Science & Engineering, Govt. College of Engineering & Ceramic Technology, Kolkata, India. He has more than 12 years of teaching experience in different engineering colleges and has published 12 research papers in different National, International Journals and Conferences. He has also successfully supervised one UGC funded research project as a Principal Investigator and his current research area includes Steganography/ Watermarking, Cryptography and Coding theory.

Nabin Ghoshal is attached with the Department of Engineering and Techn-ological Studies, University of Kalyani, West Bengal, India. He received his Ph.D. degree in Computer Science and Engineering from University of Kalyani in 2011. Dr. Ghoshal has 50 research papers in various international journals, national and international conferences. He is the author of the book titled ‘‘Steganographic Techniques and Application in Document Authentication: An Algorithmic Approach’’.