International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Digital Authentication for Wireless Domain Using Variable Marking of Multiple Secret Signatures and its Practical Implication in E-Stamp Authentication

[1]Saikat Bose, [2]Prof. (Dr.) Mohit Gangwar and [3]Dr. Tripti Arjariya[3]

Submitted: 13/09/2023 **Revised**: 18/11/2023 **Accepted**: 28/11/2023

Abstract: The work emphasizing dynamic authentications for transmitted e-documents like e-stamp paper under wireless environments through variable circular concealment of multiple invisible signature images governed by the encryption of secret key and the session random number. Additionally region wise separate bit casting strategy and dynamical bit sequencing concepts for multiple signatures ensuring greater security and robustness. Additional multi-copy signature marking on all non-overlapping areas of the document cover image, along with noticeably varied bit encoding strategies on each modified pixel byte coefficient for the cover image sub blocks, essentially improve protection and signature recovery from attacks. The reverse transformed bit coded pixel byte components for the sub blocks within the spatial domain ranges are maintained while the threshold range driven bit creation notion operates admirably under attacks. Finally, since all the secret information and the random number are likewise provided to the receiver, the securely marked signature bits may then be recognized there in the appropriate relevant ordering from the corresponding forward transformed sub block pixel byte elements. Significantly improved performance of our system in contrast to earlier efforts has been proven by significant experimental results, which also highlight solid trusted authentication and confidentiality scenarios as the key security issues.

Keywords: *E-stamp, Dynamic Authentication, Variable Signature Marking, Variable Secret Bit Coding, Region Based Multiple Watermarking.*

1. Introduction

The transmission of electronic documents, especially in the wireless sector, has become increasingly dependent on accepted authenticity verifications because to modern advancements in digital data communications [1]. Given this fact, the accepted practice to construct copyright safeguards is to disseminate secret authentic signatures as watermarks within communicated digital documents [2,3]. The goal is to securely label these signatures using trustworthy secret codes that must both prevent unauthorized detection of the signatures and ensure that they cannot be removed by various image processing assaults [2, 3].

Due to their increased security and dependability, these principles are currently being used in significantly longer variations using a variety of signature marking techniques [2, 5]. The use of such systems is primarily aimed at encouraging reliable copyright certifications through several identification phases for ownership markings and the reasonable recovery of at least one of the hidden signatures under various image processing attacks [5-8].

Three basic types of multiple watermarking concepts are described in the current literature: (a) Composite, in which all of the hidden marks are combined into a single mark that is embedded; (b) Successive, in which marks are inserted one after the other; and (c) Segmented, in which hidden marks are modulated on distinct non-overlapping portions. On these categories, composite types are more straightforward, whereas the following type provides security. However, avoiding the watermark interference problem is another significant obstacle. Both the composite and successive techniques have problems against the serious cropping attacks. This segmented version, however, offers superior robustness with the potential for at least one mark recovery during attacks [10].

In light of these potential outcomes, the suggested method actually employs numerous signature image fabrications in segmented ideas to strongly authenticate the delivered electronic documents over a wireless platform that is essentially open to unauthorised access. Furthermore, wireless communication is vulnerable to external signal interference that could seriously harm the host signal and cause severe deteriorations for any detected watermarks [4]. As a result, dynamical multi watermarking can be used to handle these situations while decent detection of at least one secret mark is given top priority.

[1]*Research Scholar, Department of Computerscience and Engineering, Bhabha University, Bhopal, Madhya Pradesh, India*
[2]*Dean (R&D), SIRT, SAGE/SIRT Group of Institutions, Bhopal, Madhya Pradesh, India*
[3]*Professor, Department of Computer Science and Software Engineering, Bhabha University, Bhopal, Madhya Pradesh, India*
**Corresponding Author Email ID: mohitgangwar@gmail.com*

2. Literature Survey

A. Related Works

Different sectors and domains for hidden data insertions can be seen in recent techniques to segment multiple watermarking. In these studies [2], a non-blind technique was developed wherein many copies of each piece of a binary copyright image were hidden on the various blue components of the host image in their encrypted form to increase robustness. Then, more recent work in [3] showed how to use a chaotic map-based technique to hide three gray scale signature images in the Red, Green, and Blue channels by encrypting both the secret bits and the positions of the corresponding markings. This pair-coupled map concept increases binary markings' security and robustness.

Recent research has been particularly concentrated on transform domain coding at various levels of the DWT components since direct manipulation of pixel bytes is generally prone to data loss and isolating secret data with ease. By coding the data on LL2 sub bands of DWT coefficients using grayscale watermarks, the work shown in [5] has emphasized good performances of the segmented concealment in comparison to the successive one. In [6], a separate segmented concept made use of several DCT energy threshold levels for the non-overlapping sub blocks to insert multiple watermarks. In fact, the research in [7] found that successive kinds of two binary images based on wavelet coefficients resulted in moderately watermarked image quality. The average watermark imperceptibility for two binary watermarks written on higher level wavelet coefficients has also been established for this type in [9]. As opposed to the work in [8], which distributed four binary images on wavelet coefficients for non-overlapping sub blocks with superior uniformity property, the current works have stressed upon embedding more watermarks through segmented types. Additionally, in [10], the results for segmented marking were superior to the previous one, which coded secret bits of two-color images on non-overlapping rows and columns of the relevant higher level wavelet coefficients. Natarajan et al. [14] highlighted about performance comparison of single and multiple water-marking techniques. In citation [15], Mohananthini et al. made comparison of multiple watermarking techniques using genetic algorithms. Again in paper [17]. Bose et al. made a Multi-Layer Digital Validation of Candidate Service Appointment with Digital Signature and Bio-Metric Authentication Approach. In other citation from [18-24] different authentication process using multiple watermarking techniques were used.

Since present literature emphasizes segmented multi watermarking in transform domain so this proposed work opts for region based dynamical multi signature fabrications through transformed coding concepts for efficient authentications.

B. Advancement on existing works

In contrast to the existing approaches this proposed work actually introduces a typical subscriber authentication protocol with dynamic fabrication of multiple signature images. This is achieved through random variations both in terms of signatures as well as respective secret signature bit sequencing concepts. Significantly this idea also injects better robustness and stronger authentications as compare to the conventional multi watermarking concepts. Apart from that the regional variations in the secret bit marking strategies applied on the cover image will further enhance the robustness and security under public wireless domain. Since the present literature study mainly stresses upon frequency domain watermarking so this proposed idea further considers a novel block transformation technique such that the secret bit will be encoded on the transformed pixel byte component of the cover image to inject extra protection for the marked signature bits. In addition distinctly separate bit encoding policies are also implemented on the transformed byte to support even better copyright preservations and robustness. In comparison to recent approaches this work also deals with four colour signature images and the colour cover image to justify very good authentication scenarios that serves superior watermark invisibility and robustness under high data payload capacity. Overall the concept conceals secret bits on all the sub-block transformed components with irregular pattern of alterations in the bit encoding parts to promote more advanced form of watermarking and authentications.

3. Proposed Dynamic Authentication

This present development is introduced in recent time to promote a new and modern health scheme based application system. This System is designed to keep in mind that subscriber e-document can be authenticated under wireless and mobile domain.

A. Subscriber Authentication Protocol

Client user first sends the authorized login id to the receiver or server while a generated random number is communicated to the client after validating the concerned user. Now client further encrypts the received random number with the secret key to produce the starting index of circular sequences for the copyright signature images. After that user invisibly marks the signature images according to this resultant sequence and based on the bit orientation cases which are derived by checking the odd or even type of the random number. Since both the random number and the secret key is also available with the receiver so the concealed signature images are successfully recovered from the received authenticated cover image. Finally the authenticity is actually confirmed based on some threshold value driven matching for these detected signatures as in Fig.1.

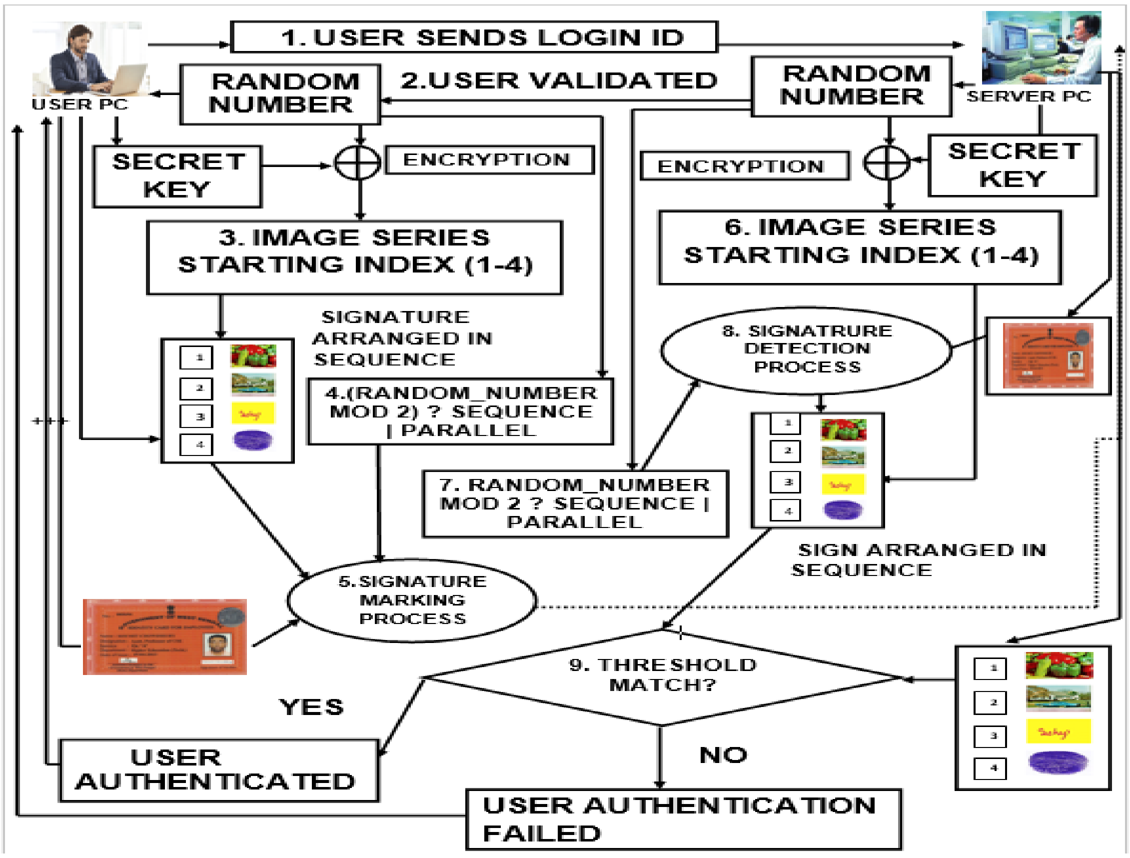


Fig 1: Authorization Technique

B. Secret Bit Orientation

The cover image is divided into four equal regions (R1, R2, R3, and R4) where each region contains non-overlapping sub-blocks of 2X2 pixel bytes where respective bit value will be stored. All four signature images are embedded in each region respectively such that the entire cover image will contain multiple copies of those signature images.

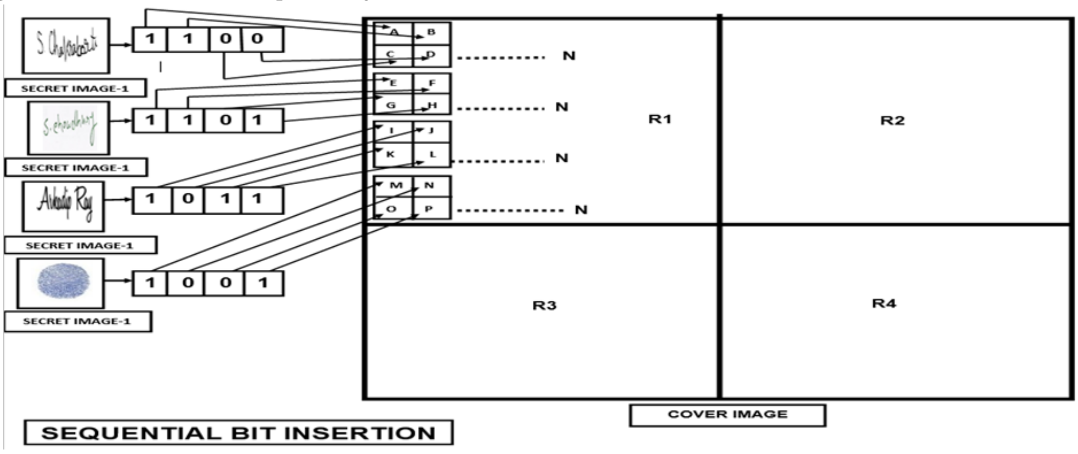


Fig 2: Sequential Bit Insertion

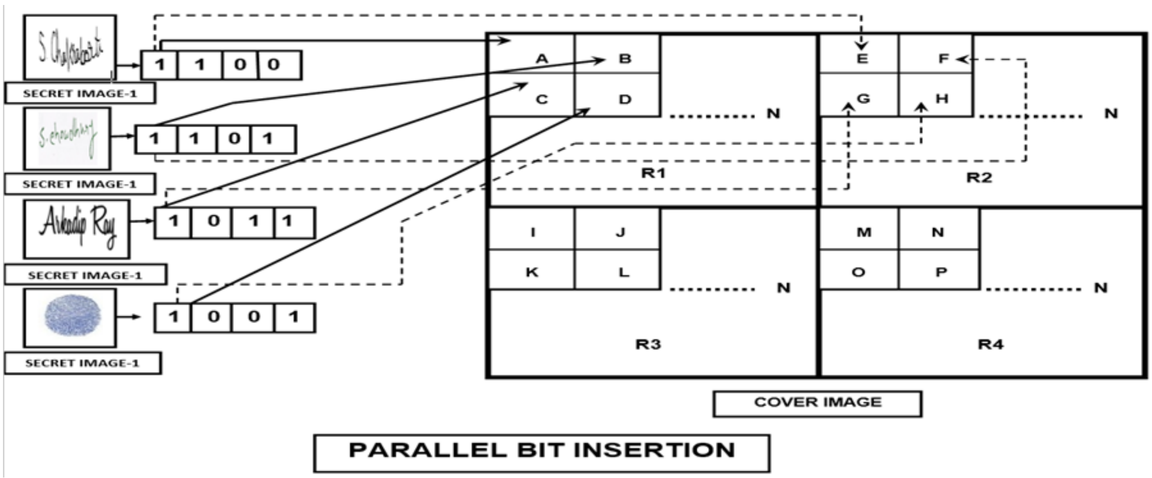


Fig 3: Parallel Bit Insertion

To impart dynamicity two types of secret bit orientations are applied as **(a) Sequential** – each sub-block pixel byte will host the bit of same signature image as shown in Fig. 2, **(b) Parallel** – each sub-block pixel byte will contain the bit of different signature image as shown in Fig. 3.

4. Signature Detection & Fabrication

The sender fabricates the cover image with signature images which are detected by the receiver. In order to achieve that bytes from secret images are integrated into cover image bytes.

A. Block Transformation Procedure

The cover image is divided into equal four regions. Each region is also divided into non-overlapping 2X2 sub-blocks of pixel bytes where respective bit value will be stored with block M= $[a_i]$, where $a_i \in \{0\text{-}255\}$, $i \in \{1\text{-}4\}$. After applying forward transformation, M block sub-matrix is

$$M_1: [A_1=(a_1+a_2)/2, A_2=(a_1 a_2)/2; A_3=(a_3+a_4)/2, A_4=(a_3-a_4)/2]$$

Further, M_1 is represented as $M_1= [A_i]$, where $A_i= [X_i+ (Y_i/2)]$ for $X_i \in \{0\text{-}255\}$, $Y_i \in \{0,1\}$, $i \in \{1\text{-}4\}$.

Secret bits are inserted into M_1 by using the possible distortion values α_i for $i \in \{1\text{-}4\}$. The resultant sub-block matrix would be $M_2= [A_i^{'}]$, where $A_i^{/}= [(X_i \pm \alpha_i) + (Y_i/2)]$ for $A_i \in \{0\text{-}255\}$, $Y_i \in \{0,1\}$, $i \in \{1\text{-}4\}$. M_2 is then inversely transformed on the previous embedded pixel values integrating corresponding fractional values which are automatically removed during the reverse transformation process. After reverse transformation new sub-matrix is generated as

$$M_3: [A_1^{//} = (A_1^{/}+A_2^{/}), A_2^{//}= (A_1^{/} - A_2^{/})\},$$

$$A_3^{//}= (A_3^{/}+A_4^{/}), A_4^{//}= A_3^{/}-A_4^{/})$$

Further, M_3 can be expressed in terms of a_i as $M_3= [A_i^{//}]$, where $A_i^{//}= [a_i \pm \alpha_1 \pm \alpha_2 \pm \alpha_3 \pm \alpha_4]$ for $A_i^{”} \in \{0\text{-}255\}$, $i \in \{1\text{-}4\}$. M_3 will then be transmitted to the receiver as watermarked sub-matrix block. Upon receiving M_3, the receiver again performs the same forward transformation to produce sub-matrix block same as M_2 which will be further operated for extraction of the secret bits hidden in pixel byte values.

B. Signature Bit Fabrication

Input: One cover & four signature images in colour format.

Output: One fabricated image containing secret images.

Method: The cover image is divided into four equal regions (R_1, R_2, R_3, and R_4) where each region contains non-overlapping sub-blocks, M of 2X2 pixel bytes that is forward transformed to M_1. Now four secret signature bits are embedded within each X_i components of M_1 and the resultant matrix, M_2 is now reverse transformed to produce the bit fabricated matrix M_3. The secret bit insertion algorithm is unique for each region with different bit insertion procedures.

Here, three procedures- Pro1, Pro2, Pro3 are optimized for bit fabrication. Let, $C_i=X_i$ and Element i ~ X_i for $i \in \{1\text{-}4\}$ where X_i is pixel value from M_1 which are fabricated according Secret signature bit, $\mu = \{0, 1\}$.

Pro1: If (C_i mod d) = 0, then $X_i = C_i$;

Else q = multiple of d nearest to C_i

where $q \leq 255$;

X_i = q; End if

Pro2: If (C_i mod d) = 0, then

If $(C_i + 1) \leq 255$, then $X_i = (C_i + 1)$;

Else $X_i = (C_i – 1)$;

Else $X_i = C_i$; End if

Pro3: If (C_i mod d) = 0,

Then L = C_i; U = (C_i + d); m = (L + U)/2; X_i = (m -1);

Else (C_i mod d)=b; L=(C_i–b);

U=(C_i+d–b); m= (L+U)/2;

X_i = (m – 1);

End if

Fabrication Method for Region R_1

For Element 1

Take d=3; If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 2

Take d=5. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 3

Take d=7. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 4

Take d=4. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

Fabrication Method for Region R_2

For Element 1

Take d=4. If μ = 1 use Pro3; Else X_i=C_i;

For Element 2

Take d=6. If μ = 1 use Pro3, Else X_i=C_i;

For Element 3

Take d=8. If μ = 1 use Pro3; Else X_i=C_i;

For Element 4

Take d=6. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

Fabrication Method for Region R_3

For Element 1

Take d=4. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 2

Take d=6. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 3

Take d=6. If μ = 1 use Pro3; Else X_i=C_i;

For Element 4

Take d=8. If μ = 1 use Pro3; Else X_i=C_i;

Fabrication Method for Region R_4

For Element 1

Take d=3. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 2

Take d=5. If μ = 1 use Pro1; Else for μ = 0 use Pro2;

For Element 3

Take d=4. If μ = 1 use Pro3; Else X_i=C_i;

For Element 4

Take d=6. If μ = 1 use Pro3; Else X_i=C_i;

C. Signature Bit Detection

Input: One Watermarked image containing secret images.

Output: Four Signatures extracted from fabricated image.

Method: First, the Watermarked image at receiver side is divided into four equal regions (R_1, R_2, R_3, and R_4) where each region contains

non-overlapping sub-blocks, M_3 of 2X2 pixel bytes which are mutually forward transformed as mentioned in Block Transformation Procedure. The resultant matrix will be similar as sub-matrix M_2 and single secret bit is recovered from M_2's frequency transformed components, X_i. Extracted bits are then properly arranged to construct four secret signatures. The signature bit extraction algorithm is unique for each region with different bit detection procedures.

Two procedures, Pro 4 and Pro 5 are used for bit detection. Let, C_i=X_i and Element i ~ X_i for i ϵ {1-4} where X_i is pixel value from M_2 which are modified according secret signature bit, μ = {0, 1}.

<u>Pro4:</u> If (C_i mod d) = 0, then μ = 1;

Else μ = 0;

<u>Pro5:</u> If (C_i mod d) = 0, then μ = 0;

Else (C_i mod d) = b; L= (C_i–b); U= (C_i+d–b);

m= (L+U)/2; n = (m – 1);

If (n = C_i) then μ = 1, else μ = 0;

Detection Method for Region R_1

For Element 1

Use Pro4 by taking d = 3;

For Element 2

Use Pro4 by taking d = 5;

For Element 3

Use Pro4 by taking d = 7;

For Element 4

Use Pro4 by taking d = 4;

Detection Method for Region R_2

For Element 1

Use Pro5 by taking d = 4;

For element 2

Use Pro5 by taking d = 6;

For Element 3

Use Pro5 by taking d = 8;

For Element 4

Use Pro4 by taking d = 6;

Detection Method for Region R_3

For Element 1

Use Pro4 by taking d = 4;

For Element 2

Use Pro4 by taking d = 6;

For Element 3

Use Pro5 by taking d = 6;

For Element 4

Use Pro5 by taking d = 8;

Detection Method for Region R_4

For Element 1

Use Pro4 by taking d = 3;

For Element 2

Use Pro4 by taking d = 5;

For Element 3

Use Pro5 by taking d = 4;

For Element 4

Use Pro5 by taking d = 6;

5. Experimental Result and Discussion

Proposed Image fabrication and detection scheme is applied on personal and standard benchmark colour images in PPM format with cover images of size 512*512 along with signature images (see TABLE I.) of size 32*32 for watermarking purposes. The work is carried out in LINUX and WINDOWS environment while the experimental data is evaluated using MATLAB R2015a, gimp 2.8, IrfanView 4.42.

A. Signature Fabrication Imperceptibility

From Table 1, it is quite evident that Watermarked images are of exact visual quality in comparison to the Original images while Table 2 reflects mostly identical

Original Image	Fabricated Image by Parallel Bit Insertion	Fabricated Image by Sequential Bit Insertion
 E-stamp		
 Plane		
 Earth		
 Lena		
 Splash		

Signature Images Used for Fabrication			
			
Fruits	House	Signature 1	Signature 2

Table 1: Images used for fabrication histograms for watermarked images basically signifying good fabricated image quality

This fact can be further satisfied by Table. 3 which shows good PSNR values in db for watermarked images indicating imperceptible hiding of secret signature bits. This table also highlights better structural similarity and correlation between pixel bytes of the Original and the Watermarked images with higher Correlation Coefficient (CC) and SSIM values close to 1. ASCII value alteration of RGB pixels is shown in Fig. 4. Then Table.4 confirms the superiority of watermark imperceptibility in comparison to the other existing approaches under high data payload capacity.

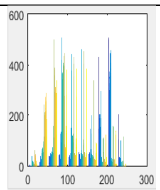
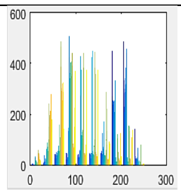
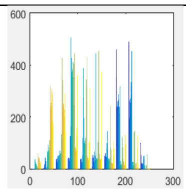
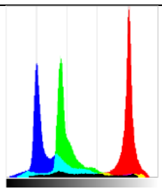
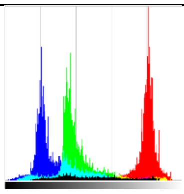
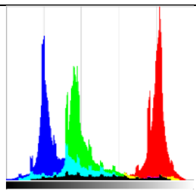
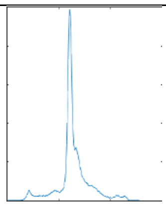
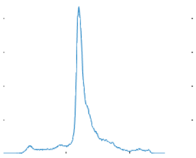
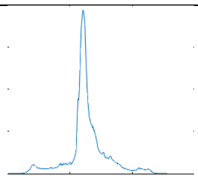
Histogram Category	**Original I-Card**	**Fabricated Image by Parallel Bit Insertion**	**Fabricated Image by Sequential Bit Insertion**
Normal Histogram			
RGB Histogram			
Normalized Histogram		 96.2 % Matched	 97.2 % Matched

Table 2: Histogram Comparison

Host Image	**Fabricated Image by Parallel Bit Insertion**			**Fabricated Image by Sequential Bit Insertion**		
I-Card	PSNR	SSIM	CC	PSNR	SSIM	CC
	40.31	0.996	0.998	38.26	0.991	0.996
Plane	PSNR	SSIM	CC	PSNR	SSIM	CC
	38.93	0.952	0.999	37.17	0.899	0.998
Earth	PSNR	SSIM	CC	PSNR	SSIM	CC
	39.06	0.993	0.999	37.62	0.984	0.998
Lena	PSNR	SSIM	CC	PSNR	SSIM	CC
	38.96	0.997	0.999	37.31	0.992	0.998
Splash	PSNR	SSIM	CC	PSNR	SSIM	CC
	38.48	0.988	0.999	37.87	0.976	0.998

Table 3: Signature Fabrication imperceptibility by PSNR, SSIM, CC

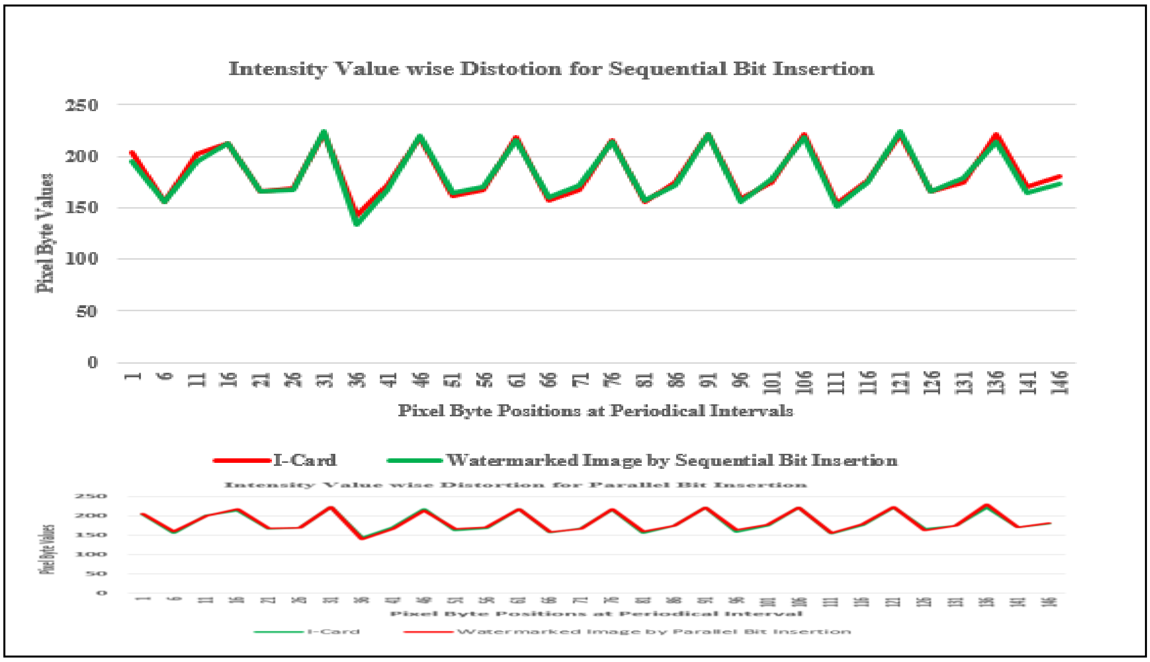


Fig 4: Intensity Value wise Distortion Graph

Applied Technique/Algorithms		Embedding Capacity (Bits or. Bytes)	PSNR (db)
Image Watermarking with Fourier Transform [12]	SCDFT	3840 bytes	30.1024
	QFT	3840 bytes	30.9283
	DCT	3840 bytes	30.4046
Multiple Watermarking Scheme on Improved Chaotic Map [3]		6144 bytes	30.11
Robust and Efficient Multiple Watermarking Scheme [6]		5120 bytes	33.8506 (max)
Robust Multi watermarking Scheme for Multi Input Digital Images [8]		4096 bits	28.44 (max)
Comparison of Multiple Watermarking Technique using Genetic Algorithm [10]		13824 bytes	38.0639 (max)
Compressive Sensing Multiple Watermarking Technique [9]		320 bytes	30.79
Proposed Approach (on E-Stamp)		49152 bytes	38.26 (min)

Table 4: Comparison of imperceptibility

B. Performance against Attack

The quality of detected signatures against attack is discussed in this section. Threshold value based secret bit encoding enhances the performance of this approach against attacks such that alterations in the pixel bytes will be evaluated on the threshold ranges during detection of bits. Performance against different attack and its comparison of attack performance is given in Fig.5 and in Table 5 respectively.

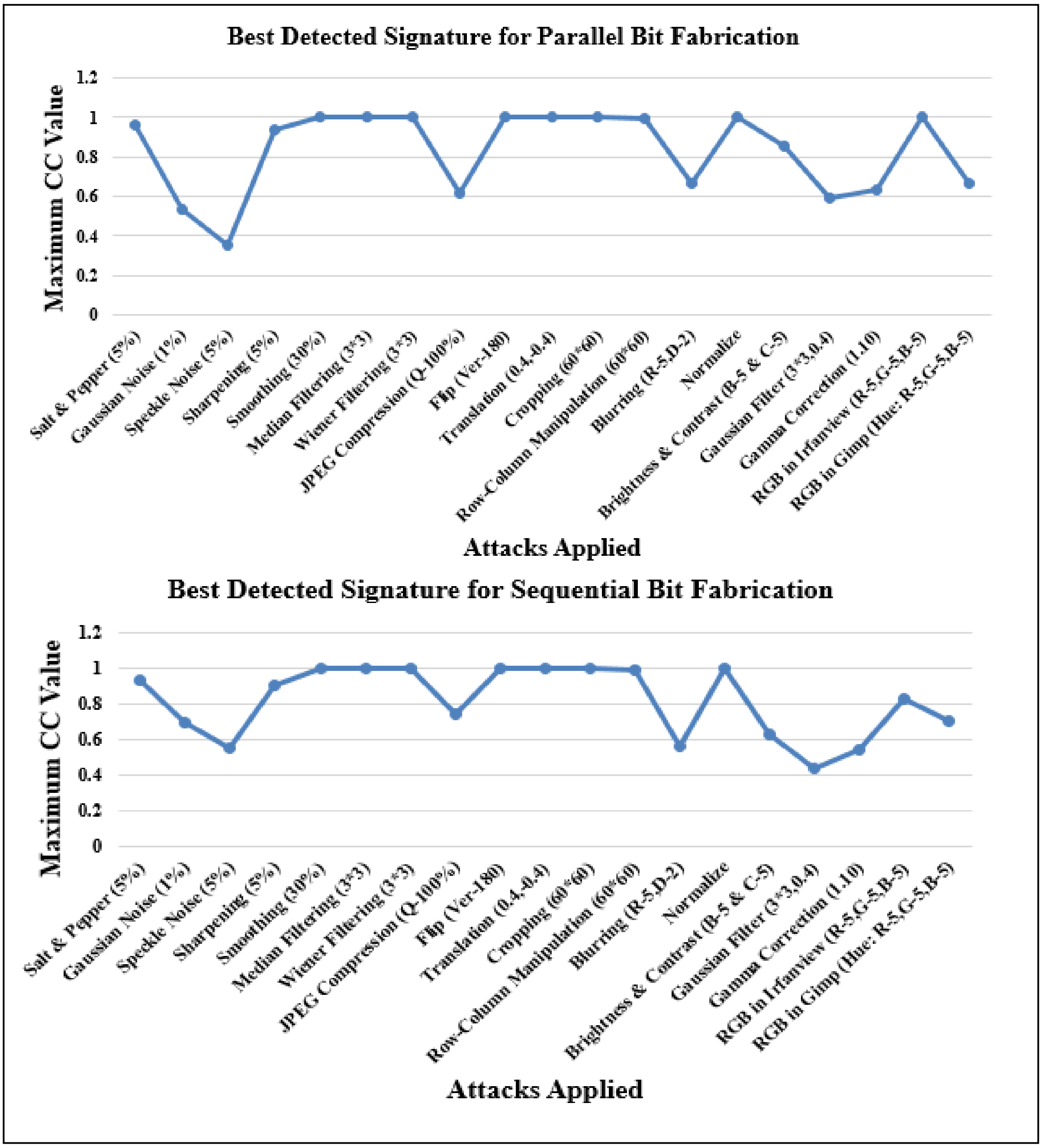


Fig 5: Performance against additional Attacks

Attack Comparison for Parallel Bit Insertion Technique						
Attack	**Attack %**	**Works**	**CC value**			
			W_1	**W_2**	**W_3**	**W_4**
Salt &	D = 10%	[13]	0.8613	0.8358	-	-

Pepper Noise (Density)	D = 5%	[7]	0.76	0.42	-	-
	D = 5%	**This Method**	**0.9534**	**0.9546**	**0.9603**	**0.9581**
Cropping (Row * Column)	-	[13]	0.6851	0.4830	-	-
	-	[10]	0.3374	0.3600	-	-
	-	[7]	0.65	0.81	-	-
	-	[2]	0.9844	0.9820	0.9716	-
	(60 * 60)	**This Method**	**1**	**1**	**1**	**1**
Trans-lation	-	[13]	0.7055	0.8141	-	-
	-	[10]	0.9586	0.9359	-	-
	-	[7]	0.35	0.99	-	-
	[0.4,0.4]	This Method	**1**	**1**	**1**	**1**
Row - Column Manipulation (Row * Column)	-	[13]	0.6860	0.6279	-	-
	-	[10]	0.6686	0.6705	-	-
	(20 * 20)	[2]	0.9898	0.9876	0.7332	
	(60 *60)	This Method	**0.9861**	**0.9869**	**0.9846**	**0.9948**
Sharpen	-	[10]	0.9078	0.9655	-	-
	-	[7]	0.92	0.99	-	-
	5 %	This Method	**0.9344**	**0.8467**	**0.8801**	**0.8589**
Smooth	-	[10]	1	1	-	-
	-	[7]	0.98	1	-	-
	30 %	**This Method**	**0.9996**	**0.9982**	**0.9982**	**0.9985**

Attack Comparison for Sequential Bit Insertion Technique

Attack	**Attack %**	**Papers**	**CC value**			
			W_1	**W_2**	**W_3**	**W_4**
Salt & Pepper Noise (Density)	D = 10%	[13]	0.8613	0.8358	-	-
	D = 5%	[7]	0.76	0.42	-	-
	D = 5%	**This Method**	**0.9254**	**0.9359**	**0.9326**	**0.9303**
Cropping (Row * Column)	-	[13]	0.6851	0.4830	-	-
	-	[10]	0.3374	0.3600	-	-
	-	[7]	0.65	0.81	-	-
	-	[2]	0.9844	0.9820	0.9716	-
	(60 * 60)	**This**	**1**	**1**	**1**	**1**

		Method				
Tran-lation	-	[13]	0.7055	0.8141	-	-
	-	[10]	0.9586	0.9359	-	-
	-	[7]	0.35	0.99	-	-
	[0.4,0.4]	**This Method**	**1**	**1**	**1**	**1**
Row - Column Manipulation (Row * Column)	-	[13]	0.6860	0.6279	-	-
	-	[10]	0.6686	0.6705	-	-
	(20 * 20)	[2]	0.9898	0.9876	0.7332	-
	(60 *60)	**This Method**	**0.9889**	**0.9923**	**0.9840**	**0.9802**
Sharpen	-	[10]	0.9078	0.9655	NE	NE
	-	[7]	0.92	0.99	NE	NE
	5 %	**This Method**	**0.9086**	**0.9025**	**0.8935**	**0.8839**
Smooth	-	[10]	1	1	-	-
	-	[7]	0.98	1	-	-
	30 %	**This Method**	**0.9998**	**0.9991**	**0.9949**	**0.9970**

Table 5: Comparison of Attack Performance

6. Practical Implication

A produced random number is communicated to the client after confirming the concerned user, and the client user delivers the authorised login id to the receiver or server first when creating an E-Stamp Paper. In order to create the initial index of circular sequences for the copyright signature images, the client now further encrypts the received random number using the secret key. The user then secretly signs the signature images in accordance with the resulting order and based on the bit orientation cases that are determined by determining whether the random number is odd or even. Fig.6 illustrates the document's elaboration.

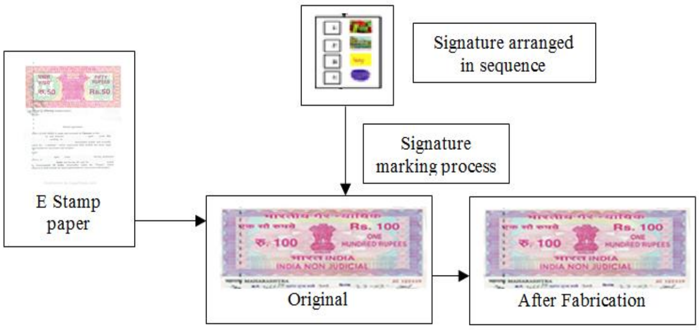


Fig 6: Document Generation

The concealed signature images are successfully recovered from the received authorized cover image since the receiver also has access to the secret key and the random number. Finally, depending on some threshold value-driven matching for these discovered signatures, the validity is actually verified. In Fig. 7, the validation procedure is depicted.

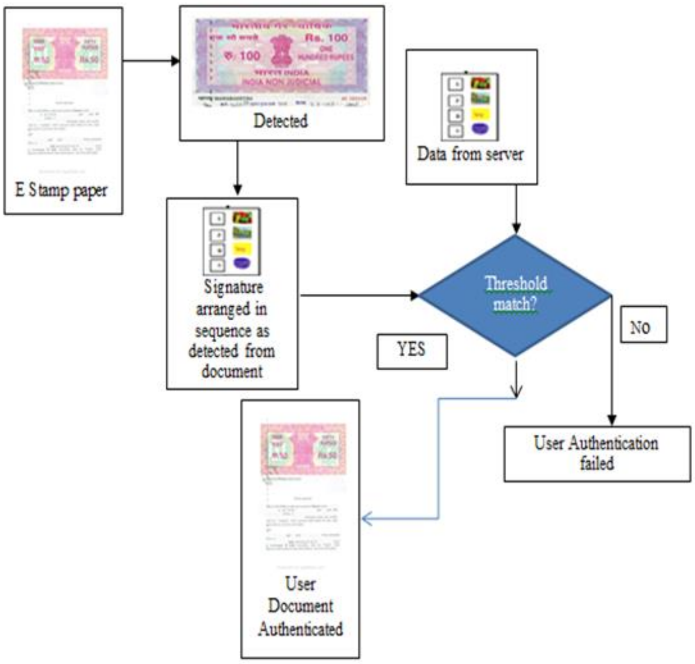


Fig 7: Document Authentication

7. Conclusion

This proposed work focusing on a novel digital authentication protocol through dynamic marking of multiple signatures both in terms of signature sequencing and its secret bit orientations. Significant enhancement in contrast to the existing schemes is achieved with region wise variable encoding of multiple copies of the secret signatures suiting wireless domain applications. Additionally unique transformation for cover image sub-blocks with different bit encoding mechanisms for the concerned pixel byte elements confirming excellent results in comparison to the existing approaches. However the concept can be upgraded for resisting the geometrical attacks and some secure signature encryption model can be incorporated for satisfying the strong authentication as well as non-repudiation aspect of security.

References

[1] T.K.Tsui, Waterloo, Xhio-ping Zhang, Androutsos D,"Color Image Watermarking using Multidimensional Fourier Transform",IEEE Trans. ON Info Forensics and Sec.,vol.3,no.1,pp.16-28,Mar 2008.

[2] Nasir, Y. Weng, J.Jiang and S. Ipson, "Multiple spatial watermarking technique in color images," Springer-Verlag London Limited, 2010 ,SIViP (2010) 4:145-154.

[3] S.Behnia,M.Teshnehlab,P.Ayubi,"Multiple-watermarking scheme based on improved chaotic maps", Elsevier B.V,2010,Common Nonlinear Sci Simulat 15(2010),pp.2469-2478.

[4] N.Ghosal, J.K. Mondal,"Discrete Fourier Transformation based Multimedia Colour Image Authentication for Wireless Communication", 2nd IEEE Intl Conf. Wireless VIATE 2011, Chennai, Feb.28 2011-March 3 2011,pp.1-5,ISBN:978-1-4577-0787-2.

[5] N. Mohananthini, G.Yamuna, R.Vivek, "Comparison of Successive and Segmented Watermarking Techniques for Colour images", NCETICT 2013, IJCA (0975-8887), 2013, pp.13–16.

[6] G.Bhatnagar and Q,M,Jonathan Wu, "A New robust and efficient multiple watermarking scheme," ,Springer Science + Business Media New York,2013,DOI 10.1007/s11042-013-1681-8.

[7] N.Mohananthini and G.Yamuna, "Performance Comparison of Single and Multiple Watermarking Techniques", vol-6, IJCNIS,DOI:10.5815/ijcnis.2014.07.04, 2014, pp. 28–34.

[8] M.Babaei,K.W.Ng,H.Babaei,H.G.Niknajeh, "A Robust Multiwatermarking Scheme for Multiple Digital Input Images in DWT Domain",vol-3,2014,IJCIT,ISSN:2279-0764,pp.834-840.

[9] R.M.Thanki,K.R.Borisagar,"Compressive Sensing

Based Multiple Watermarking Technique for Biometric Template Protection", vol,IJIGSP,DOI:10.5815.2015.01.07,2015, pp.53-60.

[10] N.Mohananthini,G.Yamuna,"Comparison of multiple watermarking techniques using genetic algorithms" ,Elsevier B.V,JESIT-70,2016.

[11] URLhttp://sipi.usc.edu/services/database/Database.html

[12] M. Kutter, F. A. P. Petitcolas, A Fair Benchmark For Image Watermarking Systems. Electronic Imaging 99, Security and Watermarking of Multimedia Contents, vol. 3657, pp. 1-14, Sans Jose, CA, USA, 25-27 January 1999, The Int. Society for Optical Engg.

[13] Mohananthini, N. & Yamuna, G., Image Fusion Process for Multiple Watermarking Schemes against Attacks. Journal of Network Communications and Emerging Technologies (JNCET), Volume 1, Issue 2, April (2015), ISSN: 2395-5317.

[14] Natarajan, M., Govindarajan, Y.: Performance comparison of single and multiple water-marking techniques. International Journal of Computer Network and Information Security. 7, 28-34 (2014). doi: 10.5815/ ijcnis.2014. 07. 04.

[15] Mohananthini, N., Yamuna, G.: Comparison of multiple watermarking techniques using genetic algorithms. Journal of Electrical Systems & Information Technology. 3, 68-80 (2016) .doi: 10.1016/j.jesit.2015.11.009

[16] Matlab:http://in.mathworks.com/help/Images/index.htm (2016).

[17] Saikat Bose, Tripti Arjariya, Anirban Goswami, Soumit Chowdhury Multi-Layer Digital Validation of Candidate Service Appointment with Digital Signature and Bio-Metric Authentication Approach International Journal of Computer Networks & Communications (IJCNC) Vol.14, No.5, September 2022DOI: 10.5121/ijcnc.2022.14506

[18] Chowdhury, S., Mukherjee, R., Ghoshal, N. : Dynamic authentication protocol using multiple signatures. Wireless Personal Communications. 93(3), 1-32 (2017). doi: 10.1007/11277-017-4066-x.

[19] Alias, N., Ernawan, F.: Multiple watermarking techniques using optimal threshold. Indonesian Journal of Electrical Engineering and Computer Science. 18(1), 368- 376 (2020). ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i1.pp368-376

[20] Liu, J., Li J., Ma, J., Sadiq, N., Bhatti, U. A., Ai, Y.: A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. Applied Sciences. 9, 700, 1- 23 (2019). doi:10.3390/app9040700.

[21] M. Gangwar, R. S. Yadav and R. B. Mishra, "Semantic Web Services for medical health planning," 2012 1st International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 2012, pp. 614-618, doi: 10.1109/RAIT.2012.6194599.

[22] Gangwar, M., Mishra, R. B., Yadav, R. S., & Pandey, B. (2013). Intelligent computing methods for the interpretation of neuropsychiatric diseases based on Rbr-Cbr-Ann integration. International Journal of Computers & Technology, 11(5), 2490-2511.

[23] Gangwar, M., Singh, A. P., Ojha, B. K., Shukla, H. K., Srivastava, R., & Goyal, N. (2020). Intelligent Computing Model For Psychiatric Disorder. Journal of Critical Reviews, 7(7), 600-603.

[24] Patil, R. S., Arjariya, T., & Gangwar, M. (2023). Detection of Cardiac Abnormalities and Heart Disease Using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 598-605.