Towards Design and Implementation of Discrete Transform Image Coding based on G-Lets and Z- transform

Intermediate report for the year 2013

Madhumita Sengupta, J. K. Mandal
Computer Science & Engineering, Faculty of Engineering, Technology & Management
University of Kalyani, West Bengal, India
e-mail: madhumita.sngpt@gmail.com, jkm.cse@gmail.com

Abstract: This article is an intermediate report submitted in partial fulfilment for the requirements of the PhD Degree in Computer Science and Engineering at the University of Kalyani for the year 2013. This article explains steganography from preliminary stage to frequency domain steganography. Two transformation techniques are used Z-Transform and G-Lets. Both this transformation techniques are explained with detail formulation, pictorial representation and practical results.

1. INTRODUCTION

Steganography is a way of writing secret messages in such a manner that no one apart from sender and intended receiver can able to identify the existence of information in secret form. Due to swift expansion in Internet, dependency on steganographic technique increases, to authenticate legal document/content and copyright protection for all digital documents. Generally secret information may be hidden in one of two ways, such as cryptography and steganography. In cryptography the information is converted into unintelligent data, where as steganography hides the presence of secret data. Cryptography encourages the intruder to break the key to decode the secret, whereas steganography don't allow intruder to suspect the secret information.

The steganographic domain is divided into four areas, such as, "data hiding", "authentication of documents and tampering detection", "secret message transmission" and "ownership protection & verification". Every domain has its own specification in respect of, quantity of data to be hidden and the degree of immunity with respect to modification of host image. These two measurements force us to increases the data to be hidden with respect to degree of immunity for host image decreases. As an example for ownership verification small amount of secret data needs to be embedded, but for secret message transmission huge amount of data needs to be hidden inside the host image.

To achieve the solution of above four problems, challenges come across the way are follows:-

a. The cover image degrades due to hidden data.
b. Hiding data into the content of the file not into the header of the file, so that hidden data must remain intact with varying header format.
c. Hiding data in spatial domain so that computation cost decreases.
d. Hiding data in frequency domain for increasing the security of hidden data inside the host image.
e. Hiding data in a manner that, any usual external forces can't temper the hidden data, such as data compression, image cropping, image rotation, Noise, ect.

The main motive of this research work is to study different transform and hiding techniques by which our four requirements can be achieved by overcoming all the challenges comes across the way, to hide the presence of the data without the observer notices, even if they are perceptible or not.

The transformation techniques studied in this phases of research are discrete wavelet transform, discrete cosine transform, and Hough transform and Daubenchies wavelet transform. Now two new transformation technique are used in steganography to get the better results. The section 2 emphasises the techniques of document authentication over Z transform domain, and section 3 defines regarding G-Let transformation technique.

2. STEGANOGRAPHY THROUGH Z TRANSFORMATION TECHNIQUE

Z-transform in signal processing converts a discrete time domain signal which is a sequence of real or complex numbers into a complex frequency domain representation. Z-transform can be defined in two ways, unilaterally and bilaterally.

In bilateral Z-transform of discrete time signal x[n] is the formal power series X(z) defined by eq (1).

$$X(z) = Z\{x[n]\} = \sum_{n=-\infty}^{\infty} x[n] z^{-n} \qquad \textbf{(1)}$$

Where n is an integer and z is, in general, a complex number.

Alternatively, in cases where x[n] is defined only for $n \geq 0$, the single dimensional or unilateral Z-transform is defined by eq(2).

$$X(z) = Z\{x[n]\} = \sum_{n=0}^{\infty} x[n] z^{-n} \qquad \textbf{(2)}$$
$$z = re^{j\omega} = r(\cos\omega + j\sin\omega)$$

Where r is the magnitude of z, j is the imaginary unit, and ω is the angle in radians. We get eq(3) by substituting the value of z in eq(2).

$$X(z) = Z\{x[n]\} = \sum_{n=0}^{\infty} x[n] r^{-n} e^{-j\omega n} \qquad \textbf{(3)}$$
$$or \qquad X(z) = Z\{x[n]\} = \sum_{n=0}^{\infty} x[n] r^{-n} (\cos\omega + j\sin\omega)^{-n}$$

On applying eq (3) for forward transformation on 2x2 mask of cover image in a row major order, four frequency component generates such as lower, horizontal, vertical and complex conjugate pair of horizontal frequency as shown in figure 1.a which is similar to subband coding. Every frequency coefficient in lower to higher frequency bands are complex number in the format of 'a + *j* b'.

Lower Frequency (LF)	*Horizontal frequency (HF)*
Vertical frequency (VF)	*Complex conjugate pair of (HF)*

(a) Z-coefficient quadrants of complex value 'a + *j* b'

Real part of LF	*Real part of HF*
Real part of VF	*Real part of HF*

(b) Real part of all frequency component 'a'

Imaginary part of LF	*Imaginary part of HF*
Imaginary part of VF	*Negation of Imaginary part of HF*

(c) Imaginary part of all frequency component '*j* b'

Fig. 1. Structural representation of coefficients of forward Z-Transform (FZT)

Every transform technique exists with pair of equations, forward and inverse. The inverse Z-transform can be obtained by eq(4).

$$x[n] = Z^{-1}\{X(z)\} = \frac{1}{2\pi j}\oint_C X(z)\,z^{n-1}\,dz \qquad (4)$$

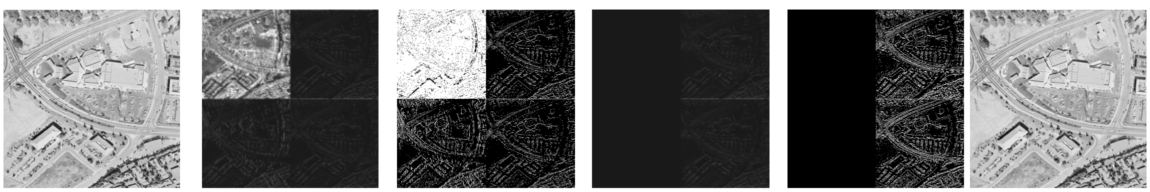
where C is a counter clockwise closed path encircling the origin and entirely in the region of convergence (ROC). A special case of this contour integral occurs when C is the unit circle. The inverse Z-transform simplifies to eq (5).

$$x[n] = \frac{1}{2\pi}\int_{-\pi}^{+\pi} X(e^{j\omega})\,e^{j\omega n}\,d\omega \qquad (5)$$

2.1 Image coding through Z-Transform with low Energy and Bandwidth (IZEB)

In this work a Z-transform based image coding technique has been proposed. The techniques uses energy efficient and low bandwidth based invisible data embedding with a minimal computational complexity. In this technique near about half the bandwidth is required compared to the traditional Z–transform while transmitting the multimedia content such as images through network.

The original gray scale image as shown in figure 2.a ‘Map.pgm’ on forward Z transform (FZT) generates four real and four imaginary subband as shown in figure 2.b and 2.d respectively. The information on the bands are emphasis through threshold as shown in figure 2.c and 2.e for real and imaginary parts respectively. Threshold increases the brightness of the small information present in the band. Inverse Z transform applied on real and imaginary parts generate lossless image back with a MSE as zero and that of PSNR is infinity.



(a) Original Map | (b) Real value after FZT | (c) Threshold Real valued part | (d) Imaginary value after FZT | (e) Threshold Imaginary part | (f) Regeneration through (IZT)

Fig. 2. Forward Z transform followed by inverse transform over image

Out of eight, four subbands are enough to regenerate lossless image at destination. This minimizes the energy and the bandwidth near to half. Further energy and the bandwidth can be reduced by reducing the subbands with little loss. Statistical calculation for loss with different numbers of subbands sent to destination to calculate image through IZT shown in table 1. It is clear from the table 1 that single band LF is enough to regenerate the image but LF needs maximum of 10 bit representation for every coefficient. And rest of all the bands need 7 to 8bit representation for coefficient.

Table 1. Statistical Data of Loss with further reduced number of subbands

Cover Image	MSE/ PSNR (db)	Number and Name of Band used to reconstruct through IZT					
		1| LF	2| LF & HF	2| LF & VF	3| LF, HF & VF	3| LF, HF & imgHF	4| LF,HF, VF & imgHF
Clock. pgm	MSE	26.827541	29.483864	41.385128	44.007004	27.010376	0.000
	PSNR	33.844995	33.434960	31.962361	31.695586	33.815497	∞

Elaine .pgm	MSE	43.429588	58.092613	62.663673	77.373775	47.226242	0.000
	PSNR	31.752946	30.489594	30.160645	29.244866	31.388970	∞
Space. pgm	MSE	12.659260	14.525913	20.651455	22.501396	13.147259	0.000
	PSNR	37.106720	36.509369	34.981297	34.608709	36.942452	∞
Tank. pgm	MSE	39.988754	53.691200	53.740608	67.420712	43.637718	0.000
	PSNR	32.111425	30.831772	30.827778	29.842870	31.732183	∞
Truck. pgm	MSE	39.040760	56.560173	48.327442	66.218987	44.382500	0.000
	PSNR	32.215621	30.605696	31.288866	29.920978	31.658686	∞

2.2 Image Authentication through Z-Transform with Low Energy and Bandwidth (IAZT)

In this work a Z-transform based image authentication technique termed as IAZT has been proposed to authenticate gray scale images. The technique uses energy efficient and low bandwidth based invisible data embedding with a minimal computational complexity. Near about half of the bandwidth is required compared to the traditional Z–transform while transmitting the multimedia contents such as images with authenticating message through network. This authenticating technique may be used for copyright protection or ownership verification. Experimental results are computed and compared with the existing authentication techniques like Li’s method, SCDFT, Region-Based method and many more based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity (IF), Universal Quality Image (UQI) and Structural Similarity Index Measurement (SSIM) which shows better performance in IAZT.

Table 2. Statistical analysis on embedding 128 x 128 dimension secret image in vertical subband/ 'Real part of VF' band, Payload 0.5 bpB.

Cover Image 512 x 512	MSE	PSNR*(dB)*	IF	UQI	SSIM
Baboon	0.502270	51.121433	0.999973	0.999904	0.999905
Boat	3.204308	43.073462	0.999831	0.999292	0.999302
Clock	0.459827	51.504855	0.999988	0.999948	0.999949
Couple	0.446041	51.637055	0.999973	0.999876	0.999878
Elaine	0.447857	51.619411	0.999978	0.999923	0.999924
Jet	0.457809	51.523956	0.999985	0.999661	0.999680
Map	0.446541	51.632192	0.999987	0.999899	0.999901
Space	0.446934	51.628372	0.999974	0.999787	0.999795
Tank	0.449867	51.599960	0.999975	0.999784	0.999792
Truck	0.451534	51.583896	0.999963	0.999781	0.999789
Average	***0.7312988***	***50.6924592***	***0.9999627***	***0.9997855***	***0.9997915***

Table 3. Statistical analysis on embedding 128 x 128 dimension secret image in horizontal subband/ 'Real part of HF' band from four minimum bands, Payload 0.5 bpB.

Cover Image 512 x 512	MSE	PSNR*(dB)*	IF	UQI	SSIM
Baboon	0.396255	52.151051	0.999979	0.999898	0.999899
Boat	0.405952	52.046052	0.999979	0.999910	0.999911
Clock	0.479259	51.325096	0.999987	0.999928	0.999929
Couple	0.404308	52.063677	0.999975	0.999848	0.999851
Elaine	0.404396	52.062734	0.999981	0.999908	0.999909
Jet	0.471886	51.392436	0.999985	0.999534	0.999561
Map	0.471886	51.392436	0.999985	0.999534	0.999561
Space	0.415325	51.946921	0.999976	0.999730	0.999740

Cover Image 512 x 512	MSE	PSNR*(dB)*	IF	UQI	SSIM
Tank	0.412228	51.979433	0.999977	0.999730	0.999740
Truck	0.413258	51.968595	0.999966	0.999729	0.999739
Average	***0.4274753***	***51.8328431***	***0.999979***	***0.9997749***	***0.999784***

Table 4. Statistical analysis on embedding 128 x 128 dimension secret image in diagonal subband/ 'Imaginary part of HF' band from four minimum bands, Payload 0.5 bpB.

Cover Image 512 x 512	MSE	PSNR*(dB)*	IF	UQI	SSIM
Baboon	0.396385	52.149629	0.999979	0.999898	0.999899
Boat	0.400246	52.107537	0.999979	0.999911	0.999912
Clock	0.455513	51.545796	0.999988	0.999932	0.999932
Couple	0.402924	52.078577	0.999975	0.999848	0.999852
Elaine	0.402523	52.082896	0.999981	0.999908	0.999910
Jet	0.474091	51.372190	0.999985	0.999532	0.999559
Map	0.404316	52.063595	0.999988	0.999875	0.999877
Space	0.409069	52.012837	0.999976	0.999734	0.999744
Tank	0.414387	51.956745	0.999977	0.999728	0.999739
Truck	0.416115	51.938672	0.999966	0.999727	0.999737
Average	***0.4175569***	***51.9308474***	***0.9999794***	***0.9998093***	***0.9998161***

Table 5. Statistical analysis on embedding 151 x 152 dimension secret image in horizontal subband/'Real part of HF' band from four minimum bands, Payload 0.7 bpB.

Cover Image 512 x 512	MSE	PSNR*(dB)*	IF	UQI	SSIM
Baboon	1.378391	46.737078	0.999926	0.999634	0.999640
Boat	1.448845	46.520585	0.999924	0.999670	0.999675
Clock	2.138859	44.828982	0.999943	0.999670	0.999673
Couple	1.532902	46.275660	0.999906	0.999408	0.999421
Elaine	1.455166	46.501679	0.999930	0.999660	0.999665
Jet	1.721626	45.771415	0.999945	0.998259	0.998357
Map	1.497513	46.377098	0.999956	0.999523	0.999532
Space	1.620136	46.035288	0.999905	0.998916	0.998957
Tank	1.457527	46.494637	0.999920	0.999016	0.999053
Truck	1.473133	46.448384	0.999879	0.999006	0.999044
Average	***1.5724098***	***46.1990806***	***0.9999234***	***0.9992762***	***0.9993017***

Table 6. Statistical analysis on embedding 151 x 152 dimension secret image in diagonal subband/'Imaginary part of HF' band from four minimum bands, Payload 0.7 bpB.

Cover Image 512 x 512	MSE	PSNR	IF	UQI	SSIM
Baboon	1.382816	46.723159	0.999926	0.999633	0.999639
Boat	1.438732	46.551004	0.999924	0.999673	0.999677
Clock	2.067417	44.976522	0.999945	0.999681	0.999684
Couple	1.538448	46.259974	0.999905	0.999406	0.999419
Elaine	1.449154	46.519659	0.999930	0.999661	0.999666
Jet	1.713501	45.791960	0.999945	0.998267	0.998365
Map	1.490669	46.396991	0.999956	0.999526	0.999534
Space	1.526279	46.294463	0.999911	0.998979	0.999018
Tank	1.460400	46.486086	0.999920	0.999014	0.999052
Truck	1.480503	46.426710	0.999879	0.999001	0.999039

Average	1.5547919	46.2426528	0.9999241	0.9992841	0.9993093

Table 7. Statistical analysis on embedding 181 x 181 dimension secret image in horizontal subband/'Real part of HF' band from four minimum bands, Payload 1.0bpB.

Cover Image 512 x 512	*MSE*	*PSNR*	*IF*	UQI	SSIM
Baboon	6.068684	40.299859	0.999673	0.998384	0.998409
Boat	6.856552	39.769746	0.999639	0.998433	0.998454
Clock	10.708042	37.833703	0.999717	0.998343	0.998358
Couple	7.724094	39.252328	0.999525	0.997007	0.997073
Elaine	6.661247	39.895248	0.999678	0.998437	0.998458
Jet	9.097958	38.541365	0.999709	0.990827	0.991339
Map	7.105892	39.614617	0.999792	0.997730	0.997772
Space	8.718529	38.726372	0.999489	0.994164	0.994385
Tank	6.680252	39.882875	0.999634	0.995477	0.995649
Truck	6.877502	39.756496	0.999436	0.995347	0.995524
Average	***7.6498752***	***39.3572609***	***0.9996292***	***0.9964149***	***0.9965421***

Table 8. Statistical analysis on embedding 181 x 181 dimension secret image in horizontal subband/'Imaginary part of HF' band from four minimum bands, Payload 1.0bpB.

Cover Image 512 x 512	*MSE*	*PSNR*	*IF*	*UQI*	*SSIM*
Baboon	6.099918	40.277563	0.999672	0.998376	0.998401
Boat	6.778450	39.819500	0.999643	0.998451	0.998471
Clock	10.442543	37.942741	0.999724	0.998384	0.998398
Couple	7.720406	39.254402	0.999526	0.997008	0.997075
Elaine	6.601910	39.934108	0.999681	0.998450	0.998471
Jet	9.111351	38.534976	0.999708	0.990814	0.991326
Map	7.102764	39.616530	0.999792	0.997732	0.997773
Space	8.015533	39.091479	0.999530	0.994632	0.994835
Tank	6.672466	39.887940	0.999635	0.995482	0.995654
Truck	6.873344	39.759123	0.999437	0.995350	0.995527
Average	***7.5418685***	***39.411836***	***0.9996348***	***0.996468***	***0.996593***

Table 9. Summarization of analysis based on different bands used for embedding with various Payload.

Calcula-tion	Real part of VF (0.5bpB)	Real part of HF (0.5bpB)	Imaginary part of HF (0.5bpB)	Real part of HF (0.7bpB)	Imaginary Part of HF (0.7 bpB)	Real part of HF (1.0bpB)	Imaginary part of HF (1.0bpB)
MSE	0.7312988	0.4274753	0.4175569	1.5724098	1.5547919	7.6498752	7.5418685
PSNR	50.692459	51.832843	51.930847	46.199081	46.242653	39.357261	39.411836
IF	0.9999627	0.999979	0.9999794	0.9999234	0.9999241	0.9996292	0.9996348
UQI	0.9997855	0.9997749	0.9998093	0.9992762	0.9992841	0.9964149	0.9964679
SSIM	0.9997915	0.999784	0.9998161	0.9993017	0.9993093	0.9965421	0.9965931

3. G- LETS BASED STEGANOGRAPHY

3.1 G-Let based Authentication/Secret Message Transmission (GASMT)

In this work a G-Let based steganographic technique, termed as GASMT has been proposed for authentication of gray scale images. The cover image transformed into one to many G-Lets based on the technique of group theory. Out of all n number of G-Lets are embedded with secret message/image for authentication. Using a secret key and a hash function watermarks/secret are embedded into few G-Let components of the cover image along with adjustment/tuning of embedded transformed G-Lets components to minimize the noise integration. Embedded G-Lets are used at the destination for authentication. Experimental results are computed and compared with the existing authentication techniques like Li's method, SCDFT, Region-Based method based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity (IF), Universal Quality Image (UQI) and Structural Similarity Index Measurement (SSIM) which shows better performance in GASMT, in terms of computational complexity with better fidelity.

The pictorial representation of forward G-let transformation over an image is shown in figure 3.

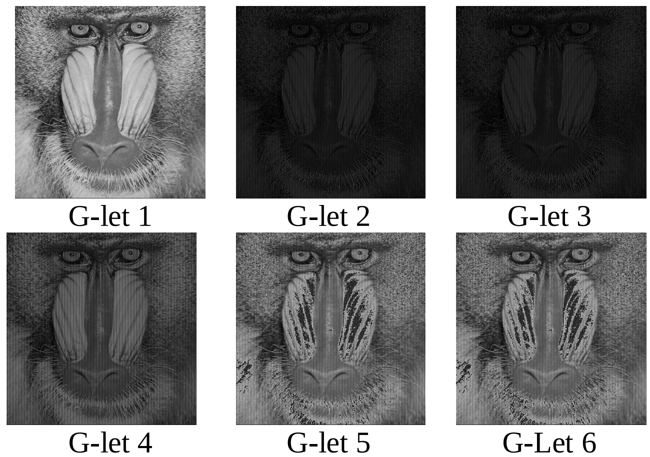


Fig 3 : Original image with six G-lets after forward transformation

Ten PGM images have been taken and GASMT is applied to obtain results. All cover images are 512 x 512 in dimension. Average of MSE for ten images is 2.6180343, PSNR is 43.951741, image fidelity is 0.999869 and that of UQI is 0.998798. All computational results for individual image are given in table 10.

Table 10. Statistical Data On Applying GASMT Over 10 Images for G-Let D_3

Cover Image	MSE	PSNR	IF	UQI
Baboon	2.617661	43.951670	0.999859	0.999305
Boat	2.618687	43.949968	0.999862	0.999404
Clock	2.673706	43.859667	0.999929	0.999588
Couple	2.637619	43.918683	0.999838	0.998981
Elaine	2.620529	43.946914	0.999873	0.999387
Jet	2.488403	44.171596	0.999920	0.997470
Map	2.628601	43.933557	0.999923	0.999161
Space	2.623821	43.941461	0.999846	0.998246
Tank	2.625320	43.938980	0.999856	0.998224
Truck	2.645996	43.904912	0.999782	0.998214
Average	***2.6180343***	***43.951741***	***0.999869***	***0.998798***

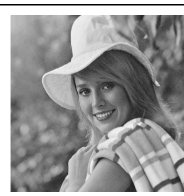
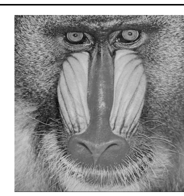
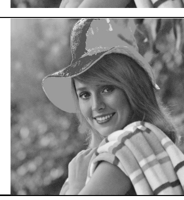
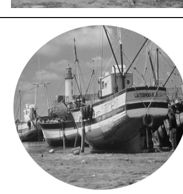
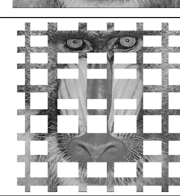
3.2 Authentication through Hough transformation generated Signature on G-Let D3 Domain (AHSG)

In this work a G-Let based authentication technique has been proposed to authenticate digital documents through Hough transform generated signature generated from original autograph. The cover image is transformed into G-Let domain to generate n number of G-Lets out of which (n/2)-1 numbers of G-Lets are embedded with secret Hough signature bits for the purpose of authentication or copyright protection. The special feature of AHSG is to optimize the distortion rate, by adjustment at the last stage of the technique, using back propagation. Experimental results are computed and compared with the existing authentication techniques like Li's method, SCDFT, Region-Based method based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity (IF), Universal Quality Image (UQI) and Structural Similarity Index Measurement (SSIM) which shows better performance in AHSG, in terms of low computational complexity and better fidelity.

Table 11: Statistical analysis on embedding 128 x 128 dimensions secret butterfly signature

Cover Image	MSE	PSNR	IF	UQI	SSIM
Baboon	1.006393	48.103126	0.999946	0.999730	0.999735
Boat	0.996788	48.144775	0.999947	0.999771	0.999774
Clock	0.998596	48.136905	0.999974	0.999845	0.999846
Couple	1.007477	48.098453	0.999938	0.999608	0.999616
Elaine	1.000916	48.126829	0.999952	0.999764	0.999767
Jet	1.020554	48.042445	0.999967	0.998956	0.999015
Map	1.002548	48.119751	0.999971	0.999677	0.999683
Space	0.997475	48.141785	0.999941	0.999327	0.999352
Tank	0.996841	48.144543	0.999945	0.999319	0.999346
Truck	0.997772	48.140490	0.999918	0.999319	0.999346
Average	***1.002536***	***48.11991***	***0.99995***	***0.999532***	***0.999548***

Attacks are the malevolent action over an image during transmission through unsecured network without prior information to the owner or concern authority. Attack is a major concern in the field of steganography. The attacks in discussion are shown in figure 4. In the first attack few windows are copied from neighbor position. Second attack is the missing of information from an image with same image tone. Third attack is on the color intensity of an object present in an image without modifying object directly. Fourth one is the common attack known as crop attack and the fifth attack is a white mesh over an image. The statistical calculation of embedded image (A) with its corresponding attacked image (B) are also shown with the extracted secret from (A) before attack and (B) after attack. The fourth and fifth attack degrade the image with MSE 4181.3 and 7247.9 respectively, after applying the authentication algorithm of proposed AHSG technique the extracted secret image can be compared with the original secret image through human perception.

	First Attack	Second attack	Third attack	Fourth attack	Fifth attack
Embedded Image (A)					
Attacked embedded image (B)					
MSE, PSNR and IF between (A) and (B)	**MSE = 145.019886 PSNR = 26.516528 IF = 0.995743**	**MSE = 287.672115 PSNR = 23.541826 IF = 0.976329**	**MSE = 605.998703 PSNR = 20.306087 IF = 0.970650**	**MSE = 4181.30521 PSNR = 11.917685 IF = 0.779188**	**MSE = 7247.904099 PSNR = 9.528679 IF = 0.609960**

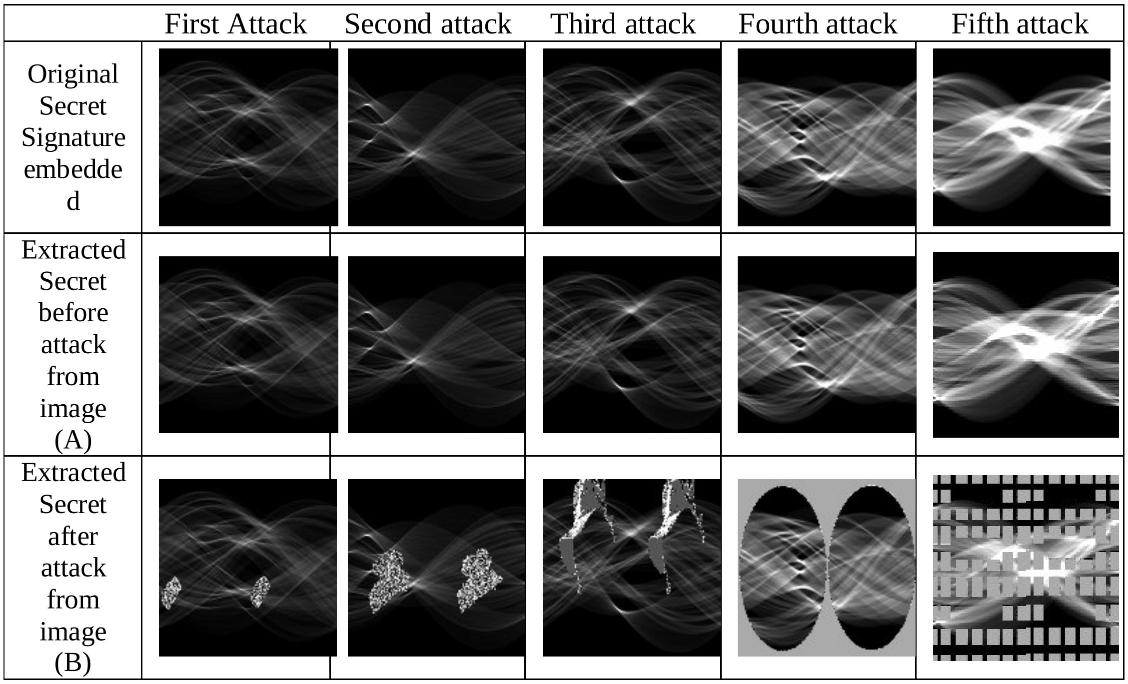


Fig. 4. Few example of attack and robust nature of the AHSG

List of Publications for the year 2013

[1] Madhumita Sengupta and J. K. Mandal, "Image coding through Z-Transform with low Energy and Bandwidth (IZEB)", The Third International Conference on Computer Science and Information Technology (CCSIT- 2013), Bangalore, India, ISSN: 1867-8211, 18-20, Feb (2013), Paper ID 182.

[2] Madhumita Sengupta, J. K. Mandal, "Image Authentication through Z-Transform With Low Energy And Bandwidth (IAZT)" , International Journal of Network Security & Its Applications (IJNSA) of AIRCC, Vol.5, No.5, pp – 43-62, DOI : 10.5121/ijnsa.2013.5504, September (2013), AIRCC Journal, Indexed by Inspec, Google Scholar, EBSCO, CSEB, Scribd, getCITED, DOAJ, pubget, CiteSeerx, .docstoc, pubZone, Ulrichs Web, WorldCat, ProQuest.

[3] Madhumita Sengupta and J. K. Mandal, "G-Let based Authentication/Secret Message Transmission (GASMT)", 4th International Symposium on Electronic System Design ISED- 2013, NTU Singapure. **(Accepted)**

[4] Madhumita Sengupta and J. K. Mandal , "Authentication through Hough transformation generated Signature on G-Let D3 Domain (AHSGD)", 1st International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA- 2013), Sponsored by AICTE, Govt. of India, Technically Sponsored by IEEE Kolkata chapter & Proceedings will be published with Procedia Technology, Elsevier, Vol. 10 (2013), ISSN 2212-0173, www.sciencedirect.com, pp – 121-130, 27th -28th September, 2013.

[5] Madhumita Sengupta, J. K. Mandal, "Hough Signature based Authentication of image through Daubechies Transform technique (HSADT)", Computer Society of India Journal of Computing, Vol. 2 , No. 1, pp- 83-89, 2013.

[6] Madhumita Sengupta, P. Mandal, Tanmoy Das and Abhijit Dey, "A Novel Hash based Technique for Thermal Image Authentication", 1st International conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA- 2013), Sponsored by AICTE, Govt. of India, Technically Sponsored by IEEE Kolkata chapter & Proceedings will be published with Procedia Technology, Elsevier, Vol. 10 (2013), ISSN 2212-0173, www.sciencedirect.com, pp – 147-156, 27th -28th September, 2013.

[7] Madhumita Sengupta and J. K. Mandal, "Color Image Authentication through Visible Patterns (CAV)", p. 617-625, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI - Volume II, Springer International Publishing Switzerland 2014, Advances in Intelligent Systems and Computing (AISC-249), Hosted by CSI Vishakapatnam Chapter, 13th -15th Dec, 2013, DOI: 10.1007/978-3-319-03095-1_67.

[8] Madhumita Sengupta, J. K. Mandal, "Steganography on Thermal Images in Wavelet Domain (STWD)", IETE Zonal Seminar on "ICT in present Wireless Revolution: Challenges and Issues (ICTWR-2013)" Organized By The Institution of Electronics and Telecommunication Engineers, Kolkata Centre, In Association With Techno Group, Salt Lake, Venue : IETE Kolkata Centre, Salt Lake; Date: 30th – 31st August, 2013.