International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 2, June-August, 2017 | Pages 36-43

Improvement of LSB Based Image Steganography

K.Srinivasan, C.Kavitha, J.Mahadevan
Dhanalakshmi Srinivasan College of Engineering and Technology, Chennai, India

Abstract - Privacy is one of the most vital troubles in modern-day conversation systems. In applications where the importance of your privateness is indispensable, the most important purpose is to send the statistics to favored target barring being captured by way of the third folks or by means of bringing them in such a way that they cannot understand. Today, researchers have developed statistics hiding methods the use of a huge range of digital media. At this point, it is necessary not only to conceal data, but additionally to develop mechanisms to stop third parties from identifying hidden data. In this study, a new technique that combine chaos-based logistic map encryption with expanded Least Significant Bit (LSB) insertion method of picture steganography used to be proposed. The message to hidden is encrypted via one dimensional logistic map and then elevated LSB technique was once used to structure stego-image. Proposed approach has been tested on three extraordinary images. Likewise, the classical LSB methods have additionally been tested on the same images. It has been viewed that proposed method multiplied the resistance of stego-images in opposition to attacks due to encryption. Additionally, Peak Signal to Noise Ratio (PSNR) in the stego-images had been elevated up to 6.6% that capability to minimize experience via the human observation. Thus, proposed method elevated the resistance and visibility of the stego-images.
Keywords - Encryption, Image Steganography, LSB, Logistic Map, PSNR.

I. INTRODUCTION

With the increasing vast use of facts technologies, work and transactions are shifted to digital environments and it will become important to defend or invulnerable the information stored, processed and transferred in these environments. In an surroundings the place digital records verbal exchange occurs, there are many threats for the message sent such as unauthorized access, damage, destruction, change and reproduction. Despite the precautions taken, reports for these threats are increasing day with the aid of day [1][2]. Various methods have been developed to get rid of these threats in response to the emergence of these threats. Encryption methods are amongst the first solutions. Encryption makes it hard to attain the original facts through changing it into an unusable form. However, there are situations in which any crypto-analysis can't be prevented. In addition, communication can be blocked with the aid of third events when it is understood that encrypted communication is made between the two aspects in the digital environment. This is the point the place the strategies of steganography take place. Steganography is a scientific self-discipline whose roots date returned heaps of years [3]. The that means of the phrase is hidden or vague writing [4]. The most primary aim is to ensure the confidentiality of the communication. In steganography, a numerical facts is saved in every other numerical data besides great changes. For example, an encrypted text is stored in an image file, and the resulting picture file is not physically and visually specific from the original. Thus, these who reveal the verbal exchange between the two aspects see a photo that is only

transferred between them, but they are not conscious that a hidden messaging in reality takes vicinity with the aid of this picture. Digital pictures are the easiest to distribute and are archives that can be met almost every web page on the internet. The most commonly used environments for steganography purposes are image files, even though they range according to the codecs used. For this reason, research on steganography and developed techniques are ordinarily in the body of photograph steganography. It is feasible to disguise a textual content inner an picture file as nicely as cover some other picture interior photograph files. Two files are concerned in embedding (or concealing) a secret information [5]. The first file, called the cover image, is the picture file that will hide the hidden information. The 2nd file is the message with the information to be hidden. This message is additionally referred to as stego. A message can be something else that can be saved as simple text, chipper text, different images, or bitmaps. As the end result of the embedding process, the cover photograph that includes the embedded message is referred to as "stego image". Information can be hidden in snap shots the usage of many distinctive methods. These methods can be grouped below two headings, taking into account the statistics they use during embedding [6].

1. Spatial / Image Domain Technique
2. Frequency / Transform Domain Technique

The method known as Spatial Domain or Image Domain uses directly the pixels of the photograph file for embedding. An instance of this approach is the Least Significant Bit Insertion (LSB) method, which is typically used. The technique recognized as Frequency Domain or Transform Domain implements embedding in cover image, which is changed in frequency domain. The algorithms for embedding statistics in JPEG structure photo archives can be proven as examples of the Transform Domain technique. These algorithms apply information embedding to the Discrete Cosine Transform (DCT) coefficients of JPEG [7].

II. RELATED WORK

In [8], a method combining Rivest-Shamir-Adleman (RSA) cryptology and LSB steganography used to be proposed. It’s finished a 5.8% increase in PSNR fee compared to the widespread LSB substitution technique.

In [9], two extraordinary LSB strategies based on bit inversion was once proposed. In the study, 6 distinctive messages have been embedded in three different images. As a result of the experiments carried out, the PSNR value used to be extended via 5.92% in first proposed method, with the aid of 15.8% in 2nd proposed method

In [10], a new LSB steganography technique was proposed for coloration images. According to this method, 2-2-4 message bits are embedded in the R-G-B channels, respectively. The new method was once experimented on 2 special photos and PSNR value was once elevated by 36.44% and 64.54%, respectively.

In [11], 1-2-4 LSB technique were applied to embed data in grayscale and shade images. The message is encrypted with the RSA algorithm to enlarge resistance in opposition to the attacks. The proposed technique was examined on four special pix and elevated PSNR cost up to 41.48% used to be obtained.

In [12], a new LSB steganography algorithm based on altering the embedding course of message bits was once proposed. The proposed method has been tested on 10 one-of-a-kind snap shots and a 1.32% enchancment in PSNR price compared to the classical LSB method has been achieved.

In [13], a new steganographic technique that combines LSB steganography with 8-Neighboring PVD (8nPVD) was proposed. The proposed new technique was once tested on 5 exclusive

images. The bought method was once compared in phrases of capacity and PSNR value. The amplify in PSNR used to be 2.38%.

III. MATERIALS AND METHODS A. LSB Technique

The least extensive bit embedding technique is a widely used and easy approach to follow [14]. In this method, the bits of the message to be hidden are placed one by means of one to least enormous bit of every byte of pixels forming cover image [15].

In this embedding process, 4 out of 8 bits have changed. However, when the embedding is executed in order, an image in which the message is hidden can be without difficulty solved via 1/3 parties. Since the identical random wide variety is possibly to be generated greater than once, there is a possibility that the same team of pixels may additionally be modified extra than as soon as in the random embedding process. In this case, personality loss can be discovered when the hidden message is solved. A simple example of this method is given in Fig 1.

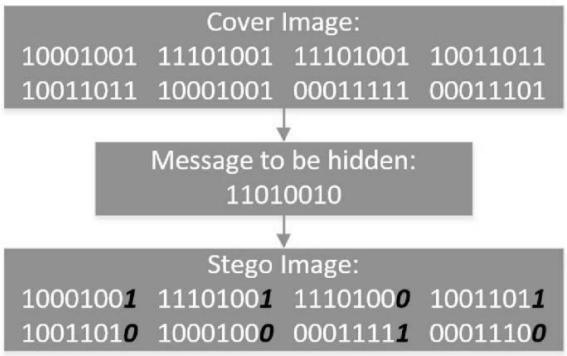


Fig. 1. An example of LSB steganography technique

B. Logistic Map

The use of chaotic indicators for carrying records was once once first put beforehand in 1993 by means of potential of Hayes et al [16]. Chaos-based encryption purposes in fact generate chaotic equations and generate a lengthy random range sequence such as pseudo-random vary turbines and encrypt a undeniable picture with this sequence [17]. One of the simplest and most studied nonlinear constructions is the logistic map. This gadget was once at the start added in 1838 by means of Pierre Franois Verhulst as a demographic model. In 1947, Ulam and von Neumann labored on the logistic map as a random wide range generator [18].

In the encoding of images, logistic maps are used in place of S-boxes due to the fact they are touchy to their preliminary conditions, behave like random number, and consist of non-repetitive features. Chaos-based encryption applications essentially encrypt the simple photograph with these random numbers by means of capability of producing a lengthy random range sequence as random variety generators the use of chaotic maps [19].

The logistic map can be formulated as in (1).

Where μ and two two are preliminary values. The map is in chaotic state when 3.57 < μ ≤4 [20], and behaves like random.

C. Image Quality Measures

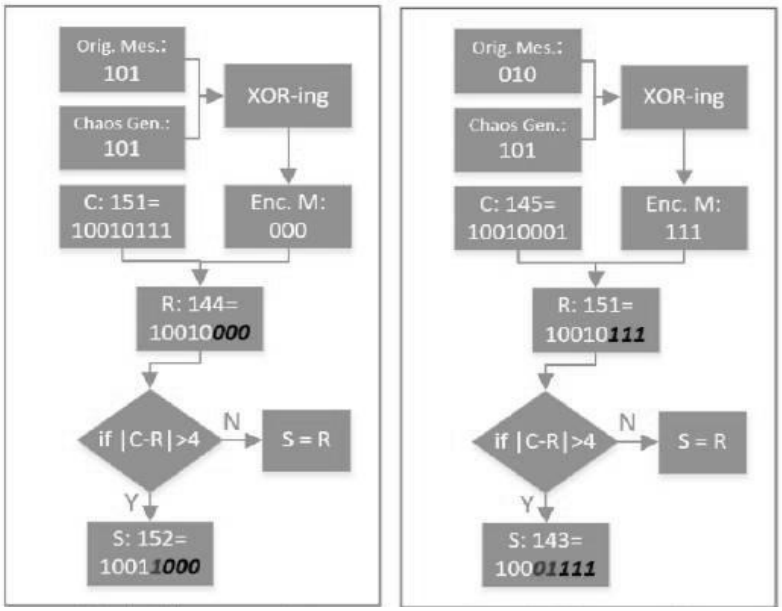
Image first-rate is a attribute for an photograph that measures the apparent image debasement (regularly, contrasted with a first-rate or perfect image). Imaging systems may additionally existing some portions of artifacts or distortion in the image, so the best assessment is an critical issue.

One of the most acquainted and broadly used measure of evaluating two pics is the Peak Signal to Noise Ratio (PSNR). PSNR is an engineering time period for the share of the most viable electrical energy of true picture to the power of the versions between proper picture and stego image. The unit of
PSNR is decibel (dB). A greater PSNR fee functionality that the stego photo is a great deal much less distorted. The Peak Signal to Noise Ratio of two snap shots can be expressed by way of (2).
Where MSE is an abbreviation of Mean Square Error and is the frequent of the difference between the proper photo and the stego image.
Another approach used to reflect onconsideration on photograph quality is Maximum Difference (MD). MD is the biggest distinction between every pixel of the special photograph and the stego image. Therefore, the lower MD value talent that the difference between the two photos can be less. The formulation for MD is given in (3).
Average Difference (AD) is each other method used in photo fantastic assessment. It is equal to suggest of the versions between unique photograph and stego image. The closer the AD rate is to 0, the increased similar the two snap shots are to every other. The method of AD is given in (4):
The Structural Similarity Index Measure (SSIM) is a perceptual metric that quantifies photograph splendid degradation brought about by using using processing such as statistics embedding or data compression. It is a full reference metric that requires two pictures from the equal photo capture: a reference image (cover image) and a processed picture (stego image). SSIM has values between zero and 1, and zero practicable that the snap pictures are surely special from every other, whereas 1 functionality that the two images are identical. The formulation of SSIM is given in (5):

IV. THE PROPOSED ALGORITHM

A. Embedding Algorithm (n-LSB on 24bit RGB image)
Using the logistic map, random numbers are produced up to the huge range of message bits to be embedded. The preliminary prerequisites x and u are used as keys in the communication. Since the chaos generator produces numbers between zero and 1, these numbers are first elevated thru 10 until the integer is reached. Then, the least significant bits of these integers are taken and used as random numbers. The encrypted message bits are bought with the resource of XOR-ing the random numbers with the authentic message bits. The least tremendous n bits of each and every pixel's R, G and B channels are sequentially modified with the bits of the encrypted message. If the big difference between the newly created R, G and B values and the genuine R, G and B values is more than 2n/2, then this distinction is decreased by; Checking and enhancing all consecutive bit opening from (n+1)th bit till the 8th bit (most magnificent bit) except it has value of 1. When the bit with price of 1 is met then exchange it’s fee to zero and stop the operation. If we have all 0s opening from (n+1)th bit to eighth bit then don’t do any trade on these consecutive bits. If the difference between the newly created R, G and B values and the original R, G and B values is a good deal less than -2n/2, then this distinction is accelerated by; Checking and enhancing all consecutive bit starting from (n+1)th bit until the eighth bit (most sizable bit) until it has value of 0 When the bit with price of 0 is met then alternate it’s rate to 1 and stop the operation. If we have all 1s beginning from (n+1)th bit to eighth bit then don’t do any alternate on these consecutive bits. When the embedding algorithm is checked, it’s been viewed that the important reason is to compensate the trade in pixel fee if it

is higher than absolute charge of 2n/2. When the alternate in pixel cost is nice and above 2n/2 the proposed strategy tries to restrict this distinction to 2n/2 that gives large PSNR price than classical n-LSB. When the change in pixel rate is horrific and less than -2n/2 the proposed approach tries to increase this distinction up to -2n/2 that also gives higher PSNR fee than classical n-LSB. An example of the embedding algorithm for 3-LSB is proven in Fig 2.



A) Embedding Example 1 B) Embedding Example 2

B. Extraction Algorithm

The least true sized three bits of every pixel of R, G and B channels of the stego photograph is fetched in order. Random numbers are generated the usage of a chaotic random range generator and preliminary values x and u. Since the chaos generator produces numbers between zero and 1, these numbers are first expanded with the resource of 10 till the integer is reached. Then, the least good sized bits of these integers are taken and used as random numbers. The original message bits are sold thru XOR-ing the random numbers with the extracted message bits. Proposed method make better complexity or resistance of stego-image in opposition to assault by means of the usage of the use of logistic map random variety generator and XOR-ing operation to encrypt the textual content message as expressed in embedding algorithm.It need to be referred to here that proposed method improves LSB via decreasing the distinction between cowl and stego-image at some stage in the embedding approach as follows: Let's take a look at how proposed method works on 3-LSB. Assume that we have 111 (3 bits) encrypted facts to embed into R channel whose final 3 bits is zero For this case the change in cover picture will be 7 (bigger than 23/2). This will have an impact on the visibility or experience of a human on the image. The proposed approach will check the 4th bit of cowl picture and if it is 1 then it will trade it to zero and then stop the operation. Changing 4th bit charge from 1 to 0 means lowering the price of associated pixel -8. Total exchange of related pixel will be 7-8=-1 as a alternative of 7 that capability to make bigger PSNR ratio of stego-image.

As can be considered from embedding-extraction algorithms proposed approach is no longer high-quality for 1-LSB. For 1-LSB, the alternate in ultimate bit can be between -1 (from 1 to 0) and 1 (from 0 to 1). The proposed method will completely follow encryption but never beautify

1-LSB due to the reality entirely the exchange in closing bit will in no way be bigger than 21/2 or that is equal to 1. Briefly speaking proposed approach totally will increase the resistance of 1-LSB due to encryption however maintain degradation of 1-LSB same. Thus, proposed technique ought to be applied to n-LSB the location n is increased than 1.

V. EXPERIMENTAL STUDY

In this study, the classical 2-LSB (last two bits insertion) and 3-LSB (last three bits insertion) methods and proposed strategies have been utilized to three exceptional photographs specifically “Lena”, “Cat” and “Bird”. These pictures are shown in Fig. three The embedding capacities of each photographs for each and every algorithm are given in Table 1. In order to see the impact of the messages in special sizes on the images, 3 text archives in first-rate sizes are used as the message. The names of these archives are “Text1.txt”, “Text2.txt” and “Text3.txt” and they have sizes of 2.71 kB, 5.82 kB and 10.48 kB, respectively. The preliminary values of the chaos generator logistic map used in this analyze about are x = 0.675 and u = 3.9762. The classical 2-LSB and 3-LSB algorithms and proposed methods had been utilized to Image 1 (Lena), Image 2 (Cat) and Image three (Bird). The acquired consequences are given in Table 2. In addition, the stego picture which is fashioned as a result of applying the proposed 3-LSB approach is given in Fig. 4 Table I. Embedding potential of every photograph in every algorithm

Methods	Capacity (Kilobyte)		
	Image 1-"Lena" 225x225	*Image 2-"Cat" 960x603*	*Image 3-"Bird" 1024x768*
2-bit LSB	37.07 Kb	423.98 Kb	576 Kb
Proposed 2-bit LSB	37.07 Kb	423.98 Kb	576 Kb

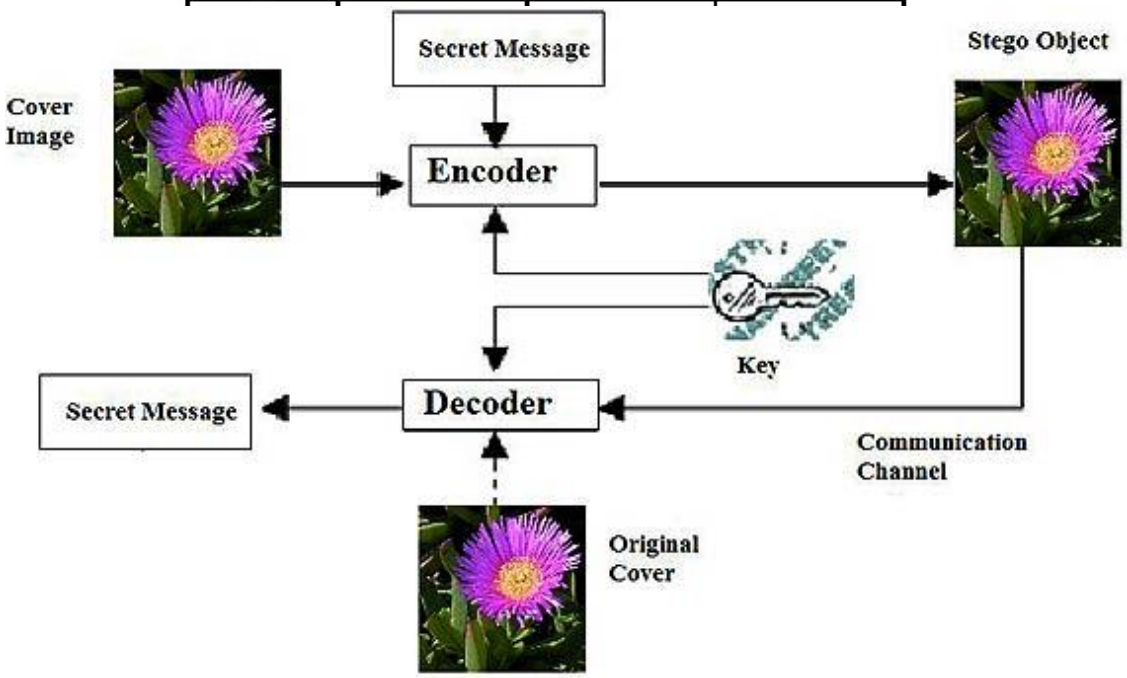


Fig. 3. Image conversion process

Table II. Embedding results

Text File	IQM	Image 1, "Lena"				Image 2, "Cat"				Image 3, "Bird"			
		2-bit LSB	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*	*2-bit LSB*	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*	*2-bit LSB*	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*
Text1.txt	PSNR	53,0082	55,2505	48,5549	51,397	63,7063	65,9110	59,1702	62,0850	65,0086	67,2403	60,5294	63,3893
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	3,1166E-	1,251E-4	0,0015	1,6461E-	1,1747E-	1,0461E-	3,4396E-	1,0096E-	6,4426E-	5,3123E-	4,0831E-	4,2244E-
	SSIM	0,9998	0,9999	0,9996	0,9998	0,999998	0,999999	0,9997	0,9998	0,999998	0,999999	0,9998	0,9999
Text2.txt	PSNR	49,7698	52,0307	45,2667	48,0838	60,5179	62,7353	56,1768	59,0674	61,8177	64,1084	57,2722	60,0947
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	2,4362e-4	4,1043E-	0,0031	6,0137E-	2,8465E-	1,8196E-	8,2132E-	1,6008E-	2,9105E-	1,2857E-	1,0808E-	3,5604E-
	SSIM	0,9995	0,9997	0,9988	0,9994	0,9997	0,9998	0,9993	0,9996	0,9999	0,9999	0,9997	0,9998
Text3.txt	PSNR	47,3333	49,5689	42,8823	45,7126	57,9943	60,1950	53,6387	56,5641	59,2513	61,5088	54,9938	57,8292
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	5,27E-05	4,8285E-	8,3182E-	4,4774E-	5,2861E-	3,2918E-	0,0016	6,7928E-	1,4355E-	9,4378E-	2,0684E-	1,1557E-
	SSIM	0,999	0,9994	0,9977	0,9988	0,9996	0,9997	0,9988	0,9994	0,9998	0,9999	0,9995	0,9997

CONCLUSION

In this paper, a new photo steganography algorithm that consists of mixture of accelerated LSB insertion and one dimensional logistic based totally absolutely (chaos theory) encryption is proposed. Traditional n-LSB algorithm is expanded by compensating the change in pixel price if it is higher than absolute cost of 2n/2. Thus, the degradation ratio between cowl and stego-images have been reduced. Proposed method has been tested on three one-of-a-kind snap shots collectively with classical 2-LSB and 3-LSB methods. three textual content material documents of one of a variety lengths had been used as the message and these messages had been encrypted with a logistic based definitely chaos generator before being embedded. The consequences received from proposed approach and classical techniques had been evaluated in accordance to the PSNR, MD, AD and SSIM criterions. The enhancements in PSNR price for every image and every textual content file are given in Table three As can be considered from Table 3, the proposed approach has PSNR values 6.6% that is greater than usual n-LSB steganography methods. Additionally, SSIM values of proposed approach had been almost identical or higher than classical n-LSB strategies as can be seen from Table 2. All these penalties showed that proposed method increases the resistance of the stego-mages besides causing substantive degradation to the cowl image.

REFERENCES

[1] Canberkoğlu, Gürol, and Şeref Sağıroğlu. Bilgi ve bilgisayar güvenliği: casus yazılımlar ve korunma yöntemleri. Grafiker, 2006.
[2] SAĞIROĞLU, Şeref, and A. L. K. A. N. Mustafa. "Her Yönüyle Elektronik İmza." Grafiker Yayınlan, Kasım (2005).
[3] Caldwell, 2nd Lt. J., “Steganography”, CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).

[4] Cummins, Jonathan, et al. "School of Computer Science." The University of Birmingham, Steganography and Digital watermarking (2004).
[5] Hartung, Frank, and Martin Kutter. "Multimedia watermarking techniques." Proceedings of the IEEE 87.7 (1999): 1079-1107.
[6] Baragwanath, Emily, and Mathieu de Bakker. Herodotus: Oxford Bibliographies Online Research Guide. Oxford University Press, 2010.
[7] Johnson, Neil F., Zoran Duric, and Sushil Jajodia. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures. Vol. 1. Springer Science & Business Media, 2001.
[8] Zhou, Xinyi, et al. "An improved method for LSB based color image steganography combined with cryptography." Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on. IEEE, 2016.
[9] Akhtar, Nadeem, Shahbaaz Khan, and Pragati Johri. "An improved inverted LSB image steganography." IEEE International Conference on Issues and challenges in Intelligent Computing techniques (ICICT). 2014.
[10] Singh, Amritpal, and Harpal Singh. "An improved LSB based image steganography technique for RGB images." Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.
[11] Goyal, Suchi, Manoj Ramaiya, and Deepika Dubey. "Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images." Computational Intelligence and Communication Networks (CICN), 2015 International Conference on. IEEE, 2015.
[12] Sugathan, Sherin. "An improved LSB embedding technique for image steganography." Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on. IEEE, 2016.
[13] Kalita, Manashee, and Themrichon Tuithung. "A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution." Systems, Signals and Image Processing (IWSSIP), 2016 International Conference on. IEEE, 2016.
[14] Esin, E. Murat, and Erdal Güvenoğlu. "Resim İçine Yazı Gizlenmesi Amacıyla Kullanılan Lsb Ekleme Yönteminin Shuffle Algoritmasıyla İyileştirilmesi." Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi 2.1 (2007).
[15] Amin, Muhalim Mohamed, et al. "Information hiding using steganography." Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.
[16] Hayes, Scott, Celso Grebogi, and Edward Ott. "Communicating with chaos." Physical review letters 70.20 (1993): 3031.
[17] Pisarchik, A. N., N. J. Flores-Carmona, and M. Carpio-Valadez. "Encryption and decryption of images with chaotic map lattices." Chaos: An Interdisciplinary Journal of Nonlinear Science 16.3 (2006): 033118.
[18] Ulam, Stanislaw M. "On combination of stochastic and deterministic processes." Bull. Amer. Math. Soc. 53 (1947): 1120.
[19] Fridrich, Jiri. "Symmetric ciphers based on two-dimensional chaotic maps." International Journal of Bifurcation and chaos8.06 (1998): 1259-1284.
[20] Bose, Ranjan, and Amitabha Banerjee. "Implementing symmetric cryptography using chaos functions." Proceedings of the 7th International Conference on Advanced Computing and Communications. 1999.