

Reversible Data Concealing in Encrypted Images using Binary- Square Embedding

Narendrababu Thumati, Kavitha Chaduvula



Abstract— The primary objective of this paper is to embed secret information using Binary-Square Embedding (BSE) technique in binary image. Using BSE, we intend to use an associate rule for Reversible Data Concealing in Encipher Images (BSE-RDCEI). This approach use BSE to implant binary bits in subordinate bit -planes of the first picture into its superior bit-planes such that the subordinate bit-planes be able to be kept back for concealing undisclosed information in resulting progression. BSE-RDCEI utilize bit- stage scrambling method when undisclosed information implant to unfold implant undisclosed information to the complete noticeable encipher image so it will forestall undisclosed information as of failure. A safety key style method is projected to reinforce the safety stage of BSE-RDCEI. Procedures of BSE-RDCEI be totally revertible. The key information & unique picture will exist remade in various ways. Examinations and correlations demonstrate that BSE-RDCEI has relate implanting rate about doubly bigger than the dynamic calculations, creates the checked decoded pictures with prime quality, and is in a situation to oppose the animal power, differential, commotion and data misfortune assaults.
Index Terms— Binary-Square , concealing, encryption, Image, Scrambling

I. INTRODUCTION

Reversible Data Concealing (RDH) has been a strategy that marginally adjusts advanced media (e.g. pictures or recordings) to insert mystery information while the first advanced media might be completely recouped with none mistake after the concealed messages are separated. It's very useful for different applications in military, bioscience or authorization, where the primary pictures or recordings mustn't be broken. Various RDH procedures were anticipated as of late. Bar diagram moving (HS) shifts numerous or the most extreme focuses in bar graph receptacles of the first picture to arrange save house for learning installing [1]. To enhance the installing ability, forecast mistake fundamentally based HS calculations were presented [2]. Developmental calculations, for example, particle swarm optimization (PSO) ,Genetic Calculation (Shieh et al)[7] and Bacterial rummaging (Huang et al)[7] are broadly utilized for information covering up. These developmental procedures are utilized to recognize coefficients of the image in change area to insert information. In any case there is an issue in finding the ideal estimations of various scaling factors (MSFs). This issue can be overwhelmed by consolidating developmental strategies with the change space procedures. Lai have joined the Genetic calculation with SVD to discover estimations of MSFs.

In any case, Loukhaoukha found that the calculation proposed by Lai caused a false positive recognition, regardless of whether the inserted watermark is unique or imaginary. Loukhaoukha et al [8] include used multi-target Ant settlement advancement in singular values deterioration utilizing lifting wavelet change (LWT SVD) space to find the estimations of MSFs. Ishtiaq et al have associated the PSO technique to find the various scaling factors in the discrete cosine change (DCT) space [2]. They use PSNR as the objective work to evaluate each atom. The noteworthy hindrance of this computation is that it so to speak revolves around the visual idea of watermarked picture without considering the force. Vahedi et al proposed a discrete wavelet change based picture watermarking methodology with atom swarm upgrade to look for perfect parameters. Li and Wang proposed a steganography technique, utilizing molecule swarm improvement calculation to discover the substitution framework also, utilized entropy coding for implanting mystery information. Here the mystery messages are changed into recurrence space before implanting into the cover image [3]. Gerami et al presented an ideal pixel change based steganography strategy alongside PSO to locate the finest area and LSB replacement for mystery information inserting. Hung et al proposed an information concealing calculation, which utilized subterranean insect province calculation to discover the substitution framework for the cover image, and the mystery information is inserted in that lattice. Bedi et al built up a PSO based information concealing plan in spatial area. In this plan, PSO finds the ideal pixel areas to implant the mystery bits in the cover image. Despite the fact that the technique results a great quality stego image, it is more helpless against different assaults amid transmission and offers a low implanting limit. Jagadeesh et al utilized solitary esteem decay edge recognition and hereditary calculation based watermarking method. This system created great superiority coding picture which is vigorous to picture preparing assaults like Low Pass Filtering[6].

TABLE I. COMPARISON OF DIFFERENT REPORTED WORKS

S. No	Technique	Payload in bits	Embedding rate (bpp)	PSNR (dB)
Spatial Domain Techniques				
1	Difference Expansion (Tian 2002)	63,66	0.243	42.86
2	HVS based (Awrangjeb &Kankanhalli 2005)	1,901	0.007	38.98
3	Histogram shifting (Ni et al 2006)	80,000	0.305	48.2

Manuscript published on 30 August 2019.

* Correspondence Author (s)

Narendrababu Thumati *, Research Scholar, JNTUK, Kakinada, Andhra Pradesh, India. tnarendrababu@gmail.com

Kavitha Chaduvula, Professor & Head, Department of IT, GEC, Gudlavalleru, A.P, India. kavithachaduvula12@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

4	Robustness Based (Ni et al 2008)	1,034	0.004	38
5	Prediction Error based (Sachnev at al 2010)	78,643	0.3	45
6	Robustness based (Zeng et al 2010)	4,096	0.016	39.11
7	Interpolation Error based (Wang et al 2013)	71,191	0.272	48.8
Frequency Domain Techniques				
8	DWT (Xuan et al 2002)	85,507	0.326	36.6
9	DCT (Lin et al 2010)	58357	0.223	34.01
10	Contourlet and SVD (Venkatanarasimhulu & Satyaprasad 2011)	256 X 256 X 8 bit Image	2	37.61
11	Slantlet Transform (Thabit & Khoo 2014)	65,536	0.25	47.03
Data Hiding based on optimization Techniques				
12	SVD-GA based (Jagadeesh et al 2010)	32 X 32 X 8 bit Image	0.0313	49.73
13	PSO based (Bedi et al 2013)	128 X 128 X 8 bit Image	0.5	45.19

II. PROPOSED METHODOLOGY

In this part, we suggest a Binary-Square embedding (BSE) procedure to implant information bits into a binary image.

A. BSE

BSE first partitions the binary images into various non-covering squares, isolates them into two gatherings named decent and terrible squares, individually. A decent square can be implanted with messages while a terrible one isn't. In message inserting stage, BSE first names the initial two or three bits of each one square with uncommon bits that demonstrate the square categories [4]. At that point the rest of the bits of a decent square resolve be supplanted through its organization data and information fragments whereas remaining of the bits of a terrible square resolve reserved unaltered. Then , we display the BSE calculation as specified .

$$c_b = \begin{cases} n - 2 & \text{for } m = 0 \\ n - 3 - p - \sum_{i=1}^m q_i & \text{for } 1 \leq m \leq n_a \\ -2 & \text{other wise} \end{cases}$$

p –payload.

q_i bits are requisite to specify ith pixel position.,

m-total bits are needed to store.

n_a threshold value.

c_b square block capacity

Square labeling points of interest are appeared in Fig.1. In this area, we suggest a BSE based revertible information stowing away calculation for encoded images (BSE-RDCEI).The structure of BSERDHEI is appeared in Fig. 2. This is made out of 3 procedures: age about scrambled

image, age about stamped encoded image, information withdrawal / image recuperation.

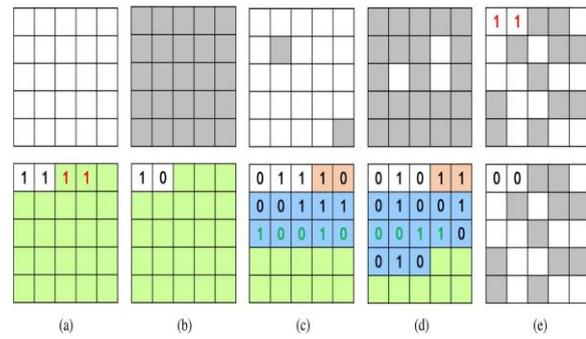


Fig. 1. BSE with the areas of order 5 X 5. The 1st and 2nd columns show the five sorts of extraordinary squares and their contrasting embedded outcomes. White and diminish boxes address the pixels with estimations of 1 and 0, separately. The colored regions are utilized to embed payload in the Square.(a) and (b) are Decent-I and Decent-II deters through Cb = 23 and their introduced results;(c) Decent-III square with Cb = 10 and its embedded outcome; (d) Decent-IV upset with Cb = 7 and its introduced outcome; and (e) horrendous square with Cb = 2 and its result in the wake of inserting.

These techniques are refined by the substance proprietor who gives the principle picture, the information protector who has the riddle information to be implanted and the specialist, autonomously. The substance proprietor utilizes the BSE tally to implant joined bits of lesser piece planes of the fundamental picture trapped on its raised piece planes with a definitive target that its lower bit-planes can be held for covering riddle information in the succeeding systems. It is encoded utilizing the image encipher key KI [5]. The information encodes the question information utilizing the information encipher key KD, embeds them into the held lower bit-planes in the encoded picture, and scrambles the image utilizing the distribution encipher key KS to make the ventured encoded picture which resolve convey in excess of open channels. The particular 3 encipher keys are emotionally made by clients.

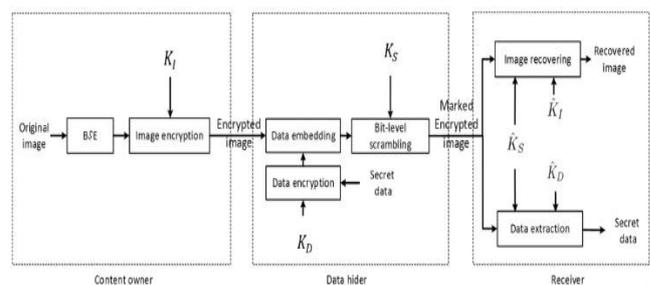


Fig. 1. Architecture of the suggested methodology.

B. The message revival and image recouping

The message encryption and image recouping incorporates two stages: stage 1 Payload recovery and decent square recouping. Stage 2 terrible square recouping. In stage1, the BSE filters the initial 3 naming bits of each one square to decide the square kind. For a decent square, BSE removes parameter m, the areas of m pixels and payload bits local the square & afterward recreates the square dependent on extricated data.

Something else, for a terrible square, BSE records the square file. In stage 2, BSE recoups the initial 2 pixels of every terrible square utilizing the removed payload and keeps the rest pixels unaltered.

C. Random key sequence generation

The BSE-RDCEI requires key generation to perform image encryption, data encryption, and bit-level scrambling .It uses random key sequence generation, HMAC(Hashed Message Authentication Code) algorithm and their structure is appeared in Fig. 3.

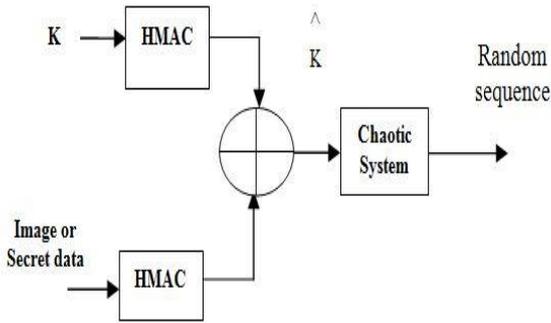


Fig. 2. Secure key generation

Hashed Message Authentication Code (HMAC) is utilized to create two arbitrary hash digests with the contributions of client indicated secret key K and picture/mystery information, separately. At that point the EX-OR two hash digests are to create the inward irregular grouping to generate key.

RESULTS

BSE finds with identical regions, modifies the identical regions, and edges will be kept as it is. These tasks capitulate an image with more commotion. Fig. 4 demonstrates the implanting after effects of four 512 by 512 double images utilizing the BSE calculation with the square size of 4 by 4. As we can observe, the extra every white or every single dark square in the first image contains, the most inserting rate BSE can accomplish. In the mean time, the inserted images turn out to be more clamors like. To examine the installing rate, we concern BSE with various square sizes to 9,000 double test metaphors are produced by binaries the dim scale images as of BOWSBaSe1 with the edge ascertained by Otsu’s strategy [2]. Table II records the normal inserting speed of all test images through various square orders. At this time take $s1 = s2$. From the outcomes, we can see that, the normal inserting rate achieves the greatest esteem when the square size is 7 by 7. At the point when square size is under 7 by 7, the normal installing rate increments with the square size expanding, and it diminishes when square size is bigger than 7 by 7. BSE familiarizes confusion with uniform zones, turn the systematic territories, and stock only the edges. These undertakings outturn a picture with numerous upheaval. As we can front, the more all-white or each dull square the primary picture encompass the over embedding rate BSE can attain. In the interim, the implanted images turn out to

be more commotion like. Fig. 5 outwardly demonstrates the connection between the edge n_a and square pixel number n .

TABLE II. MEAN EMBEDDING RATE USING BSE WITH DIFFERENT SQUARE SIZES

Square size $s \times s$	Average embedding rate r (.bpp)	Square size $s \times s$	Average embedding rate r (.bpp)
3 by 3	1.8379	9 by 9	2.149
4 by 4	2.1948	11 by 11	2.0216
5 by 5	2.2134	12 by 12	1.8466
6 by 6	2.1762	14 by 14	1.8967
7 by 7	2.1774	17 by 17	1.9831
8 by 8	2.1575	20 by 20	1.7874



Fig. 3. Results of the proposed methodology.

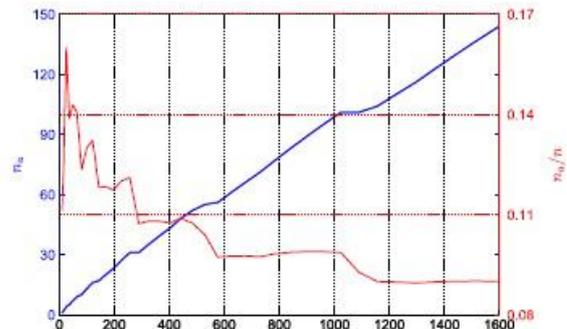


Fig. 4. Threshold Vs Square pixel number n

III. CONCLUSION

In this article, anticipated a Binary Square Embedding (BSE) system for embedding correspondence in parallel pictures. Given BSE, we have proposed reversible information covering in encoded pictures (BSE-RDCEI) in which BSE is used in support of saving the bit space for embeddings mystery information. BSE-RDCEI utilizes improved dimension scrambling process after riddle information inserting to spread implanted secret information to the whole ventured blended picture.



A safety key agreement segment is anticipated to upgrade its protection intensity. Both BSE and BSE-RDCEI are contained ended up being revertible. Reenactments and connections have gave the idea that BSE-RDCEI beats further current procedures to the extent the introducing rate and PSNR outcome of the unscrambled pictures. Defense investigation has exhibited the heartiness of BSE-RDCEI in contrary to diverse assaults.

REFERENCES

1. Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol. 16 (3) (2006) 354362.
2. J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol. 13 (8) (2003) 890896.
3. A. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process. 13 (8) (2004) 11471156.
4. H.-J. Kim, V. Sachnev, Y.Q. Shi, J. Nam, H.-G. Choo, A novel difference expansion transform for reversible data embedding, IEEE Trans. Inf. Forensics Secur. 3 (3) (2008) 456465.
5. D. Coltuc, J.-M. Chassery, Very fast watermarking by reversible contrast mapping, IEEE Signal Process. Lett. 14 (4) (2007) 255258.
6. X. Wang, X. Li, B. Yang, Z. Guo, Efficient generalized integer transform for reversible watermarking, IEEE Signal Process. Lett. 17 (6) (2010) 567570.
7. Huang, HC Yueh-Hong Chen Ajith Abraham 2010, Optimized Watermarking Using Swarm- Based Bacterial Foraging, Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 1, pp. 51-58
8. Loukhaoukha, K, Chouinard, JY Taieb, MH 2011, Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization, Journal of Information Hiding and Multimedia Signal Processing, vol.2, no.4, pp.303-319.
9. Gerami, P, Subariah, I Morteza, B 2012, Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment International Journal of Computer Applications, vol. 55, no. 2, pp. 20-25.
10. Jagadeesh, B, Srinivas Kumar, S Raja Rajeswari, K 2010, Image watermarking scheme using singular value decomposition, quantization and genetic algorithm, International Conference on Signal Acquisition and Processing, pp. 120-124.

AUTHORS PROFILE



Mr. T. Narendra Babu is a research scholar at department of Computer Science and Engineering at JNTU Kakinada. He completed M.Tech in JNTU Anantapur, India. He has qualified lectureship in Andhra Pradesh State Eligibility Test (APSET) in 2014, qualified UGC NET in 2018 conducted by National testing Agency (NTA) for lecturer ship he got AIR 861 in GATE 2006. He was awarded as Best Teacher in 2013. He is having 10 years of teaching experience in under graduation courses. His areas of interest are Cryptography & Network Security, Image Processing, Mobile Computing and Algorithms. He has published 3 papers in International Conferences, 7 papers in International Journals.



Dr. Kavitha Chaduvula is a professor and head of Information Technology Department at Gudlavalluru Engineering College. She completed Ph.D from JNTU Kakinada. She is a life member in ISTE, IE and institute nominee member in CSI. She has 18 years of teaching experience. She published 14 papers in International Journals, 10 papers in international and national conferences. She guided 20 under graduated projects and 5 post graduate projects. Her research interests include Image Processing, Pattern Recognition and Machine Learning.