International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 3269–3275

# A Novel Message-based Watermarking using Blind Source Separation and 7D Hyper-Chaotic Map

[0000-0003-0982-9424]**Anil Kumar**, [0000-0001-9047-3693]**PriyankaDahiya**

DIT University, Dehradun, INDIA
dahiyaanil@yahoo.com
dahiyapriyanka814@gmail.com

**Abstract.** We present a novel arrangement of message-based watermarking using a blind source segment and a 7D Hyper-chaotic map. Watermark, a message first converted using Hadamard code, protects from various attacks compared to the ASCII input. The interpreted watermark is encoded by precise blending. The encoded watermark is embedded in spread-range style into the main unearthly segments of the picture utilizing help pseudo-irregular grouping to make the watermark non-defenseless against the assault of a functioning interloper or because of clamor in the transmission interface. Test results show that this framework is functioning admirably in a fuzzy climate.

**Keywords:**Blind source separation (BSS), Watermarking, Hadamard codes, Spread Spectrum, and SOM.

## 1.1 Introduction

In the current time of PCs and quick correspondence, one must shield copyright proprietorship from an unapproved client through any electronic media. For this reason, the computerized watermark is utilized as the distinguishing proof code that is for all time covered up inside the picture. The watermarking technique ought to have perceptual straightforwardness, strength, comprehensiveness, limit, payload, and unambiguousness.

G. J. Yu [1] proposes watermarking,a message in nature;for this situation,the watermark is encoded before concealing the information inside the picture. This strategy is different defenseless sorts of assaults.

Lin et al. [2-7] present the idea of utilizing blind source division (BSS), which is successfully cryptanalysis by Kumar et al. [8]. Kumar et al. [9-11] have proposed various BSS techniques.

Turner [12], Koch et al. [13, 14] given various for Watermarking. Satish et al. [15] used the spread spectrum technique.
Here, a novel strategy proposed watermarking utilizing blind source detachment and spread method used visually impaired source partition procedure for scrambling the message for information covering up.

## 1.2 BASIC OF 7D Hyper-Chaotic Map

It is using 1-nonlinear and 2-linear feedback controllers because of the highly random. It is used for cryptography.



ISSN: 2233-7857 IJFGCN

$$v_1' = s(v_2 - v_1) + v_4 + ev_6 \quad 1(a)$$

$$v_2' = pv_1 - v_2 - v_1v_3 + v_5 \quad 1(b)$$

$$v_3' = -tv_3 + v_1v_2 \quad 1(c)$$

$$v_4' = ev_4 - v_1v_3 \quad 1(d)$$

$$v_5' = -iv_2 + v_6 \quad 1(e)$$

$$v_6' = lv_1 + mv_2 \quad 1(f)$$

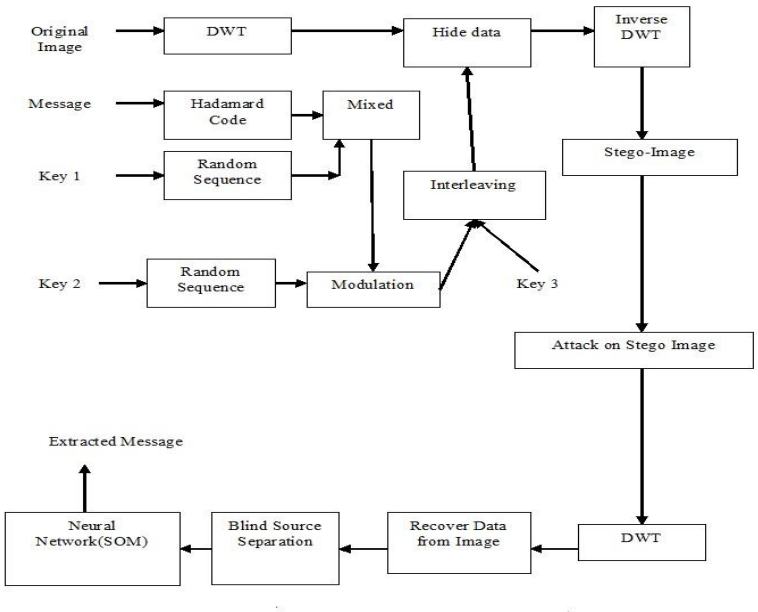
$$v_7' = gv_7 + nv_4 \quad 1(g)$$

Where $v_1, v_2, v_3, v_4, v_5, v_6, and v_7$ are initial state variables.$n$is coupling parameter, $s, t, and p$ are constant, $r, e, i, l, m, and g$ are control parameters.

## 1.3 Proposed Method

The proposed plot has appeared in Figure 1, which is made out of the installing framework.

**Fig. 1.**Proposed modelArchitecture




Random number generated using 7D Hyper-chaotic map, using the following Algorithm 1.


ISSN: 2233-7857 IJFGCN

**Algorithm 1:** Pseudorandom sequence generator using 7D Hyper-Chaotic Map

**1.** Begin

**2.** Iterate of Eq. (1) eight times of the hidden info; the pseudorandom is formed as $[1], XKey, XKey, XKey, XKey, XKey, and\ XKey$.

**3.** for i= 1 to $2 * size\ of\ the\ secret\ d$

$$X1(i) = \lfloor XKey[1](i) * 2 \quad 2(a)$$

$$X2(i) = \lfloor XKey[2](i) * 2 \quad 2(b)$$

$$X3(i) = \lfloor XKey[3](i) * 2 \quad 2(c)$$

$$X4(i) = \lfloor XKey[4](i) * 2 \quad 2(d)$$

$$X5(i) = \lfloor XKey[5](i) * 2 \quad 2(e)$$

$$X6(i) = \lfloor XKey[6](i) * 2 \quad 2(f)$$

$$X7(i) = \lfloor XKey[7](i) * 2 \quad 2(g)$$

**4.** end

Non-straight Hadamard code encodes the message (m) that givesthe most extreme standard hamming distances.Encode data is mixed using key X1, message m' is produced and modulated utilizing Key 2. The following sign s previously interleaved utilizing key 3 for forestalling an explosion of mistakes presented by the interloper/assailant and further embedded into the cover picture by considering energy proficient wavelet strategy.

## 1.4 EXPERIMENTAL RESULT AND PERFORMANCE ANALYSIS

In the current examination, the accentuation is given to the essential information embedded in the image to adjust straightforwardness, vigor, and limit. These boundaries rely upon the size and intricacy of the picture inside which the watermark is installed. Aside from this, it likewise relies on the capacity of the image.

It is expected that the Human limit esteem is embraced, and the Wlength coefficients can be utilized to install the watermark in the picture. Then, the most extreme length of the information that can be covered up inside the picture can be acquired by utilizing the condition (1) given underneath.

$$\frac{W_{length}}{2 \times 512} \qquad (1)$$

The worth 512 is for the length of the Hadamard code. The limit of the information storedis.

$$\frac{W_{length} \times 8}{2 \times 512} \qquad (2)$$

Presently, the piece mistake rate can be diminished by expanding the length of the Hadamard code, yet it builds the intricacy of the neural organization and diminishes the number of characters embedded in the cover picture.



ISSN: 2233-7857 IJFGCN

## Experimental results

Take a 24-bit Lena image (1024 x 1024) as the cover image, leading to $W_{length}$ =1048,,576. Hence, at most, 1024 characters can be hidden inside the Lena image ref equation (1).

Here different sorts of assaults perform on the Stego-picture. We increase hiding data size and also noise to check the results.

Table I first consider 30 characters to be hidden, changing the percentage of the noise; we have considered uniform, salt, Gaussian, and speckle noise and calculated the average percentage of the error. Testing was performed 1000 times. Figure 2 shows the result.

**Fig. 2.Error when we embedded 30 Characters**

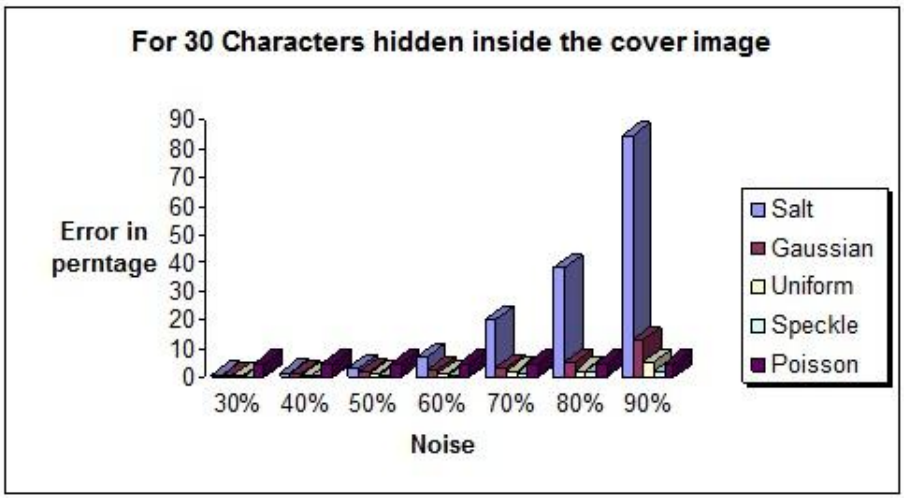



**TABLE I. 30 CHARACTER AS MESSAGE**

| Noise | Uniform | Poisson | Salt | Gaussian | Speckle |
|---|---|---|---|---|---|
| 30% | 0.49 | 4.81 | 0.82 | 0.66 | 0.16 |
| 40% | 0.66 | 4.81 | 1.48 | 1.32 | 0.33 |
| 50% | 1.12 | 4.81 | 3.06 | 1.98 | 0.49 |
| 60% | 1.28 | 4.81 | 6.83 | 2.64 | 0.49 |
| 70% | 2.11 | 4.81 | 19.9 | 2.97 | 1.48 |
| 80% | 2.14 | 4.81 | 38.3 | 5.28 | 1.65 |
| 90% | 4.98 | 4.81 | 84.5 | 12.7 | 1.98 |

Tables2,3,4, and 5 for 100, 200, 300, and 400 characters watermark, respectively.


ISSN: 2233-7857 IJFGCN

**TABLE II.** 100 CHARACTER AS MESSAGE

| Noise | Salt | Gaus-sian | Uni-form | Speckle | Pois-son |
|---|---|---|---|---|---|
| 30% | 1 | 0.5 | 1 | 0.5 | 10 |
| 40% | 4 | 4 | 2 | 0.6 | 14 |
| 50% | 5 | 6 | 2 | 0.7 | 14 |
| 60% | 24 | 7 | 3 | 1.5 | 15 |
| 70% | 27 | 9 | 4 | 1.8 | 18 |
| 80% | 65 | 12 | 7 | 1.9 | 19 |
| 90% | 80 | 13 | 9 | 3 | 20 |

**TABLE III.** 200 CHARACTER AS MESSAGE

| Noise | Salt | Gaus-sian | Uni-form | Speckle | Pois-son |
|---|---|---|---|---|---|
| 30% | 2 | 3 | 2 | 1 | 22 |
| 40% | 4 | 4 | 3 | 1 | 22 |
| 50% | 6 | 6 | 4 | 1 | 22 |
| 60% | 9 | 7 | 5 | 1.5 | 22 |
| 70% | 30 | 9 | 6 | 2 | 22 |
| 80% | 66 | 13 | 8 | 4 | 22 |
| 90% | 83 | 14 | 10 | 5 | 22 |

**TABLE IV.** 300 CHARACTER AS MESSAGE

| Noise | Salt | Gaus-sian | Uni-form | Speckle | Pois-son |
|---|---|---|---|---|---|
| 30% | 4 | 4 | 3 | 2 | 33.2 |
| 40% | 5 | 5 | 4 | 2 | 33.2 |
| 50% | 6 | 6 | 4 | 2 | 33.2 |
| 60% | 15 | 7 | 6 | 3 | 33.2 |
| 70% | 35 | 11 | 8 | 4 | 33.2 |
| 80% | 70 | 14 | 10 | 4 | 33.2 |
| 90% | 84 | 15 | 12 | 6 | 33.2 |



ISSN: 2233-7857 IJFGCN

TABLE V. 400 CHARACTER AS MESSAGE

| Noise | Salt | Gaus-sian | Uni-form | Speckle | Pois-son |
|---|---|---|---|---|---|
| 30% | 5 | 5 | 4 | 4 | 44.4 |
| 40% | 6 | 6 | 7 | 4 | 44.4 |
| 50% | 10 | 12 | 12 | 5 | 44.4 |
| 60% | 20 | 15 | 14 | 6 | 44.4 |
| 70% | 40 | 16 | 10 | 7 | 44.4 |
| 80% | 80 | 18 | 12 | 9 | 44.4 |
| 90% | 90 | 20 | 15 | 10 | 44.4 |

## 1.5 Conclusion & Summary

An epic message-based watermarking has been proposed utilizing enormous hamming code, daze source partition, turbulent tweak, interleaving, and wavelet change. This gives protection from clamor present in the channel and any gatecrasher. The security execution of the framework is principally improved. This technique itself is modest in execution and subsequently can be utilized securely in business consumer items adequately.

## References

1. G. J. Yu, C. S. Lu , M. Liao , A message-based cocktail Watermarking System, Pattern Recognition 36 (2003) 957-968.
2. Lin Qiu-Hua, Yin Fu-Liang. Blind source separation applied to image cryptosystems with dual encryption. Electron Lett 2002;38(19):1092–4.
3. Lin Qiu-Hua, Yin Fu-Liang. Image cryptosystems based on blind source separation. Proc Neural Networks Signal Process 2003;2:1366–9.
4. Lin Qiu-Hua, Yin Fu-Liang, Zheng Yong-Rui. Secure image communication using blind source separation. In: Proceedings of the IEEE sixth circuits and systems symposium on emerging technologies: frontiers of mobile and wireless communication, vol. 1, 2004. p. 261–4.
5. Lin Qiu-Hua, Yin Fui-Liang, Mie Tie-Min, Liang Hua-Lou. A speech encryption algorithm based on blind source separation. In: International conference on communications, circuits and systems (ICCCAS), vol. 2, 2004. p. 1013–7.
6. Lin Qiu-Hua, Yin Fu-Liang, Mei Tie-Min, Liang Hualou. A blind source separation based method for speech encryption. IEEE Trans Circuits Syst I2006;53(6):1320–8.
7. Lin Qiu-Hua, Yin Fu-Liang, Mei Tie-Min, Liang Hualou. A blind source separation-based method for multiple images encryption. Image Vision Comput2008;26:788–98.
8. Anil Kumar, RhoumaRhouma, Yong Wang, Nicolas Sklavos, M.K.Ghose, Comments on, "A blind source separation-based method for multipleimages encryption", Commun Nonlinear SciNumerSimulat 16 (2011) 1675–1686.


ISSN: 2233-7857 IJFGCN

9. Anil Kumar, E. A. Elkhazmi, Othman O Khalifa, AbdulganiAlbagul, Secure Data Communication Using Blind Source Separation, Proceedings of the International Conference on Computer and Communication Engineering, May 13-15, 2008 Kuala Lumpur, Malaysia:1352-56.
10. Anil Kumar, M. K. Ghose, An Improved Secure Data Communication UsingBlind Source Separation and Chaos, Proceedings of 2009 11th IEEE International Symposium on Multimedia, USA :358-62.
11. Anil Kumar, M. K. Ghose, K. V. Singh, An Extended Secure Data Communication UsingBlind Source Separation and HC-128, Proceedings of 2010 IEEE 2nd International Advance Computing Conference:201-05.
12. L. F. Turner, Digital data security system, Patent IPN WO 89/08915, 1989.
13. E. Koch, J. Rindfrey, and J. Zhao, Copyright protection for multimedia data, in Proc.Int. Conf. Digital Media and Electronic Publishing, 1994.
14. E. Koch and J. Zhao, Toward robust and hidden image copyright labeling, in Proc. 1995 IEEE Workshop on Nonlinear signal and Image Processing, June 1995.
15. K. Satish, T. Jayakar, Charles Tobin, K. Madhavi, and K. Murali, Chaos Based Spread Spectrum Image, IEEE Transactions on Consumer 588 Electronics, Vol. 50, No. 2, MAY 2004:587-90.
16. A.Kejariwal, S. Gupta, A.Nicolau,N. D. Dutt, R. Gupta, IEEE Transactions On Very Large Scale Integration (VLSI) Systems, vol. 14, no. 6, June 2006:625-36.


ISSN: 2233-7857 IJFGCN