S. Smys
Abdullah M. Iliyasu
Robert Bestak
Fuqian Shi *Editors*

New Trends in Computational Vision and Bio-inspired Computing

Selected works presented at the ICCVBIC 2018, Coimbatore, India

Springer

New Trends in Computational Vision and Bio-inspired Computing

S. Smys • Abdullah M. Iliyasu • Robert Bestak
Fuqian Shi
Editors

New Trends in Computational Vision and Bio-inspired Computing

Selected works presented at the ICCVBIC 2018, Coimbatore, India

Springer

Editors
S. Smys
Department of CSE
RVS Technical Campus
Coimbatore, TN, India

Abdullah M. Iliyasu
Tokyo Institute of Technology
School of Computing
Tokyo, Japan

Robert Bestak
Department of Telecommunication Engineering
Czech Technical University in Prague
Prague, Czech Republic

Fuqian Shi
College of Information Science & Engineering
Wenzhou Medical University
Wenzhou, China

ISBN 978-3-030-41861-8 ISBN 978-3-030-41862-5 (eBook)
https://doi.org/10.1007/978-3-030-41862-5

Mathematics Subject Classification (2020): 65D19, 68Uxx, 68T05, 92-08, 92Bxx

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

We are honored to dedicate the proceedings of ICCVBIC 2018 to all the participants and editors of ICCVBIC 2018.

Foreword

It is with deep satisfaction that I write this Foreword to the Proceedings of the ICCVBIC 2018 held in, Coimbatore, Tamil Nadu, on 29–30 November 2018.

This conference was bringing together researchers, academics, and professionals from all over the world, experts in Computational Vision and Bio-inspired Computing.

This conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. The papers contributed the most recent scientific knowledge known in the field of Computational Vision, Fuzzy, Image Processing, and Bio-inspired Computing. Their contributions helped to make the conference as outstanding as it has been. The Local Organizing Committee members and their helpers put much effort into ensuring the success of the day-to-day operation of the meeting.

We hope that this program will further stimulate research in Computational Vision, Fuzzy, Image Processing, and Bio-inspired Computing and provide practitioners with better techniques, algorithms, and tools for deployment. We feel honored and privileged to serve the best recent developments to you through this exciting program.

We thank all authors and participants for their contributions.

Coimbatore, India — S. Smys

Preface

This Conference Proceedings volume contains the written versions of most of the contributions presented during the conference of ICCVBIC 2018. The conference provided a setting for discussing recent developments in a wide variety of topics including Computational Vision, Fuzzy, Image Processing, and Bio-inspired Computing. The conference has been a good opportunity for participants coming from various destinations to present and discuss topics in their respective research areas.

ICCVBIC 2018 Conference tends to collect the latest research results and applications on Computational Vision and Bio-inspired Computing. It includes a selection of 179 papers from 505 papers submitted to the conference from universities and industries all over the world. All of accepted papers were subjected to strict peer-reviewing by 2–4 expert referees. The papers have been selected for this volume because of quality and the relevance to the conference.

ICCVBIC 2018 would like to express our sincere appreciation to all authors for their contributions to this book. We would like to extend our thanks to all the referees for their constructive comments on all papers, especially, we would like to thank the organizing committee for their hard working. Finally, we would like to thank the Springer publications for producing this volume.

Coimbatore, India　　　　Abdullah M. Iliyasu

Acknowledgments

ICCVBIC 2018 would like to acknowledge the excellent work of our conference organizing the committee, keynote speakers for their presentation on 29–30 November 2018. The organizers also wish to acknowledge publicly the valuable services provided by the reviewers.

On behalf of the editors, organizers, authors, and readers of this conference, we wish to thank the keynote speakers and the reviewers for their time, hard work, and dedication to this conference. The organizers wish to acknowledge Dr. Smys, Dr. Joy Chen, Dr. R. Harikumar, and Dr. Jude Hemanth for the discussion, suggestion, and cooperation to organize the keynote speakers of this conference. The organizers also wish to acknowledge speakers and participants who attend this conference. Many thanks are given for all persons who help and support this conference. ICCVBIC would like to acknowledge the contribution made to the organization by its many volunteers and members who have contributed their time, energy, and knowledge at a local, regional, and international level.

We also thank all the Chair Persons and conference committee members for their support.

Contents

3-Dimensional Multi-Linear Transformation Based Multimedia Cryptosystem

S. N. Prajwalasimha

1 Introduction

As the technology nurtures, different cryptanalysis techniques are being introduced, in order to crack the cryptographic algorithms [1–3]. Presently most of the existing systems are composed of different permutation and substitution methods [4, 5]. Even though the key length is more, it will be a quite greater combinations for the brute force attacker to find the secrete key and to cryptanalyze the algorithm with the help of high speed super computers [6, 7].

Now a day, communication system requires high level security and authentication [8–13]. Chaos theory of randomness has been adopted by many cryptographic algorithms. These chaotic maps are used to generate random numbers for substitution. During cryptanalysis, attacker exercises on all possible chaotic generators for different combinations of key to decrypt the information. Algorithmic complexity can be further increased by number of rounds, but it is a matter of time for the attacker to perform cryptanalysis on the algorithm. Sensitivity to the initial conditions is a major parameter of chaotic systems. Based on the above parameters, the popular chaotic maps such as: 3D Baker map, 3D Arnold's cat map and Logistic map are adopted for cryptography [14, 15]. Inter pixel redundancy in the images will be high. Hence the correlation between the adjacent pixels is strong and that should be reduced as high as possible in the cipher image [16–18].

Based on the above facts, a new chaotic transformation technique has been introduced, which is 3-dimensional, discrete and real. Moreover the above transformation is reversible, so that to retrieve a loss less decrypted information.

S. N. Prajwalasimha (✉)
Department of Electronics and Communication, ATME Research Centre, Mysore, Karnataka, India

S. Smys et al. (eds.), *New Trends in Computational Vision and Bio-inspired Computing*, https://doi.org/10.1007/978-3-030-41862-5_1

2 Three Dimensional Multi Linear Transformation (3D-MLT)

Let f: $S \rightarrow S$ be a 3-dimensional chaotic map.

Where, S is phase space (3-dimensional cube or 3-dimensional torus).

Let F_M be a chaotic cryptographic primitive such that

$$F_M : \{0, 1, \ldots .M-1\}^3 \rightarrow \{0, 1, \ldots .M-1\}^3$$

For large values of M, F_M approximates f

$$f\left(x^|, y^|, z^|\right) = \left\{\left(x + (\delta\text{-}1)\,y + (\rho\text{-}1)\,z\right) \bmod 2^n, \left(x + \delta y + (\rho\text{-}1)\,z\right) \bmod 2^n, \left(x + (\delta\text{-}1)\,y + \rho z\right) \bmod 2^n\right\}$$
$$x, y, z < 2^n$$
$$\delta, \rho < 2^n \tag{1}$$

where $x^|$ is the first dimensional equation
$y^|$ is the second dimensional equation
$z^|$ is the third dimensional equation
n is the information size (Bits)
x is the first initial condition
y is the second initial condition
z is the third initial condition
δ and ρ are the primary constants

In the above plot it can be clearly observed that, the randomness of the derived samples is not linear and changes greatly with very small variations in the initial conditions. From Fig. 1 it can be concluded that the proposed transformation technique is very sensitive to the initial conditions, so that it is very difficult to predict the derived samples.

2.1 *Inverse 3D-MLT*

Consider Eq. (1)

$$f\left(x^|, y^|, z^|\right) = \left\{\left(x + (\delta\text{-}1)\,y + (\rho\text{-}1)\,z\right) \bmod 2^n, \left(x + \delta y + (\rho\text{-}1)\,z\right) \bmod 2^n, \left(x + (\delta\text{-}1)\,y + \rho z\right) \bmod 2^n\right\}$$

where

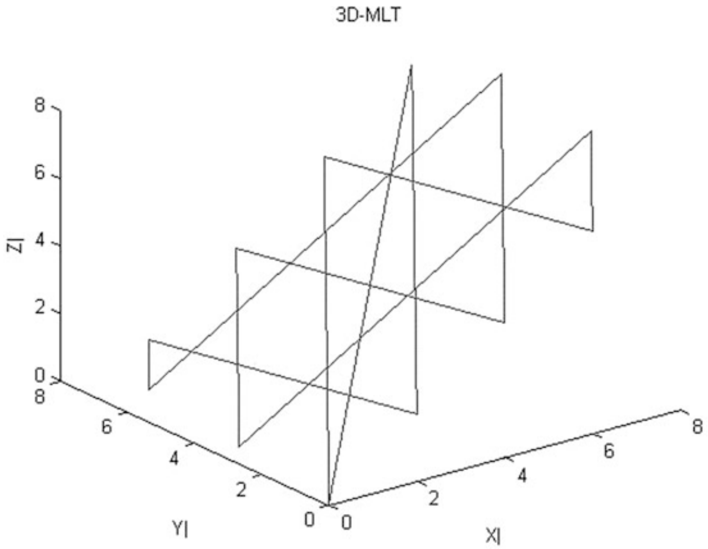

Fig. 1 Plot of 3D-MLT with initial conditions

$$x^{|} = x + (\delta\text{-}1)\, y + (\rho\text{-}1)\, z \tag{2}$$

$$y^{|} = x + \delta y + (\rho\text{-}1)\, z \tag{3}$$

$$z^{|} = x + (\delta\text{-}1)\, y + \rho z \tag{4}$$

Subtracting Eq. (2) from (3) we get,

$$y = y^{|}\text{-}x^{|} \tag{5}$$

Subtracting Eq. (2) from (4) we get,

$$z = z^{|}\text{-}x^{|} \tag{6}$$

Substituting Eqs. (5) and (6) in (2) we get,

$$x = \left\{(\delta + \rho\text{-}1)\, x^{|} + (1\text{-}\delta)\, y^{|} + (1\text{-}\rho)\, z^{|}\right\} \tag{7}$$

Equations (5), (6) and (7) give the inverse 3D-MLT

$$y = \left(y^{|}\text{-}x^{|}\right) \bmod 2^{n} \tag{8}$$

$$z = \left(z^{|}\text{-}x^{|}\right) \bmod 2^{n} \tag{9}$$

$$x = \left[\left\{ \left(\left(\delta + \rho\text{-}1 \right) x^{|} + \left(1\text{-}\delta \right) y^{|} + \left(1\text{-}\rho \right) z^{|} \right) \right\} \bmod\ 2^{\mathrm{n}} \right] \tag{10}$$

Equations (8), (9) and (10) represent inverse 3D-MLT for bounded state space.

3 Proposed Scheme

In the proposed algorithm, encryption is done in two phases: Transformation (Mapping) phase and Substitution (Saturation) phase.

3.1 Transformation (Mapping) Phase

Transformation phase involves mapping of each pixel position in the host image to get cipher image of first stage, which is also termed as 3D-MLT image of host. The same process is carried out for secrete image and the resultant transformed images of both host and secrete images are subjected to logical XOR operation to get the cipher image of second stage. The transformation phase performs the following steps:

Step 1: The host image is subjected for 3D-MLT.

$$h^{|} \left(p^{|}, \mathrm{q}^{|} \right) = h \left(\left\{ \left(x + \left(\delta\text{-}1 \right) y + \left(\rho\text{-}1 \right) z \right) \bmod\ 2^{n}, \left(x + \delta y + \left(\rho\text{-}1 \right) z \right) \bmod\ 2^{n} \right\} \right) \tag{11}$$

The initial values consider here are,

$$\delta = 4,\ \rho = 1$$

$$\mathrm{n} = 8$$

$$h^{|} \left(p^{|}, \mathrm{q}^{|} \right) = h \left(\left\{ \left(x + 3y \right) \bmod\ 256, \left(x + 4y \right) \bmod\ 256 \right\} \right) \tag{12}$$

where h is the host image.
$h^{|}$ is the 3D-MLT image of host.

Step 2: The secrete image is also subjected for 3D-ML transformation.

$$s^{|}\left(p^{|},\mathrm{q}^{|}\right)=s\left(\left\{\left(x+\left(\delta\text{-}1\right)y+\left(\rho\text{-}1\right)z\right)\bmod\ 2^{n},\left(x+\left(\delta\text{-}1\right)y+\rho z\right)\bmod\ 2^{\mathrm{n}}\right\}\right) \tag{13}$$

The initial values consider here are same as that of the host image,

$$\delta=1,\ \rho=5$$

$$\mathrm{n}=8$$

$$s^{|}\left(p^{|},\mathrm{q}^{|}\right)=s\left(\left\{(x+4z)\bmod\ 256,\ (x+5z)\bmod\ 256\right\}\right) \tag{14}$$

where s is the secrete image.
$s^{|}$ is the 3D-ML transformed image of secrete.

Step 3: The resultant transformed images of both host and secrete are subjected for logical XOR operation pixel wise.

$$r\left(p,q\right)=h^{|}\left(p^{|},\mathrm{q}^{|}\right)\oplus s^{|}\left(p^{|},\mathrm{q}^{|}\right) \tag{15}$$

where r is the cipher image of second stage.

3.2 Substitution (Saturation) Phase

Substitution phase comprises of S-box of size $2^{\mathrm{n}}\times 1$, which consists of 256 bits secrete key. The secrete key is subjected for first set of initial permutation and then inserted into the S-box at specified locations. The remaining values in the S-box are.

pre-defined and pre-specified. The obtained cipher image of second stage is subject for pixel wise logical XOR operation along with S-box in the row wise manner.

$$r^{|}\left(p,q\right)=r\left(p,q\right)\oplus S-box \tag{16}$$

where $r^{|}$ is the cipher image of third stage or cipher image of first round (Fig. 2).

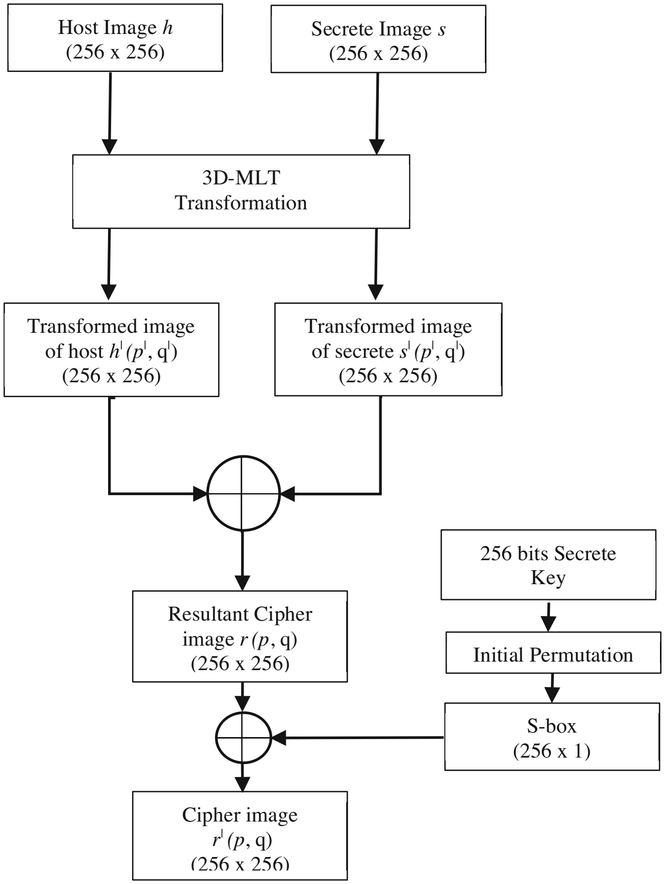

Fig. 2 Flow diagram of proposed encryption algorithm

3.3 Decryption Phase

Step 1: The obtained cipher image from second stage is logically XORed with the elements of S-box created by secrete key. The resultant image is the decrypted image from the second stage.

$$r\left(p,q\right)=r^{|}\left(p,q\right)\oplus S\text{-}box \tag{17}$$

Step 2: The secrete image is subjected for 3D-ML transformation for the same set of initial values as implemented in the encryption stage.

$$s^{|}\left(p^{|}, q^{|}\right) = s\left(\left\{\left(x + (\delta\text{-}1)\, y + (\rho\text{-}1)\, z\right) \bmod 2^{n}, \left(x + (\delta\text{-}1)\, y + \rho z\right) \bmod 2^{n}\right\}\right)$$

The initial values consider here are same as that of the host image,

$$\delta = 1, \rho = 5$$

$$n = 8$$

$$s^{|}\left(p^{|}, q^{|}\right) = s\left(\left\{(x + 4z) \bmod 256, (x + 5z) \bmod 256\right\}\right)$$

where s is the secrete image.
$s^{|}$ is the 3D-ML transformed image of secrete.

Step 3: The decrypted image from the first step is logically XORed with the transformed image from the second step to get the resultant image of the host in the transformed form.

$$h^{|}\left(p^{|}, q^{|}\right) = r\,(p, q) \oplus s^{|}\left(p^{|}, q^{|}\right) \tag{18}$$

Step 4: The resultant image from the above step is subjected for inverse 3D-ML transformation to get the desired original image.

$$h\,(x, y) = h^{|}\left(\left\{\left((\delta + \rho\text{-}1)\, p^{|} + (1\text{-}\delta)\, q^{|} + (1\text{-}\rho)\, r^{|}\right) \bmod 2^{n}\right\}, \left(q^{|}\text{-}p^{|}\right) \bmod 2^{n}\right\}\right) \tag{19}$$

The initial values consider here are,

$$\delta = 4, \rho = 1$$

$$n = 8$$

$$h\,(x, y) = h^{|}\left(\left\{\left(4p^{|}\text{-}3q^{|}\right) \bmod 256, \left(q^{|}\text{-}p^{|}\right) \bmod 256\right\}\right) \tag{20}$$

where h is the host (Original) image.
$h^{|}$ is the 3D-ML transformed image of host.

Table 1 Comparison mean square error and correlation between original and decrypted images with LSB neutralization attack

Images	MES	Correlation
Lena	4.4948	0.9763
Baboon	3.4061	0.9685
Peppers	3.8869	0.9764

4 Experimental Results

Matlab software is used for the implementation. Three standard images are considered for the analysis with a substitution image. Table 1 describes the mean square error (MSE) and correlation between original and decrypted images showing very minimum MSE. The correlation is almost equal to one indicating the original and decrypted images are similar to each other under least significant bit (LSB) neutralization attack (Tables 2, 3, and 4).

5 Conclusion

In the proposed cryptosystem, a new three dimensional chaotic transformation technique is designed and implemented, showing the effective random behavior for different initial conditions. By the above transformation technique, the correlation between the adjacent pixels have been effectively broken and more entropy is achieved by the cipher image, when compared with other existing cryptosystems which are implemented by making uses of some more popular chaotic transformation techniques. The algorithm is designed with two levels of security. The key length used by the algorithm is 256 bits, by that 2^{256} combinations makes the level of difficulty high for the brute force attacker. Even though the key combination is made by the attacker, it is very difficult to decrypt the information, since it requires the secrete images at the first stage per each round, which is unknown for the attacker and hence it is hard to cryptanalyze the algorithm. The obtained cipher image is subjected to security tests such as unified average changing intensity (UACI), number of pixel change rate (NPCR) and mean square error rate (MSE). The results obtained are better compared to the existing algorithms. The security level can be further increased by increasing the size of the S-box and number of rounds in the algorithm.