Sl. No.	Authors	Title of the Paper	Name of the Journal	Indexed (SCI/Scopus/WoS	Volume and issue No.	Year	Impact Factor
1.	PP Devi, B Jaison	Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms	Computer Communications	SCIE	152	2020	2.816
2.	M Tamil Selvi, B Jaison	Lemuria: A Novel Future Crop Prediction Algorithm Using Data Mining	The Computer Journal	SCIE	https://doi.org/10.1093/comjnl/bxaa093	2020	1.077
3.	S Mohamed Sulaiman, B Jaison, M Anto Bennet	Design Of Low Power 16 Bit Counter With Programmable Combinational Logic And Integrated Clock Gating Using 16NM Technology	International Journal of Electronics	SCIE	https://doi.org/10.1080/00207217.2020.1793398	2020	1.004
4	K Sundara Krishnan, B Jaison, SP Raja	An Efficient Novel Color Image Encryption Algorithm based on 3D Lu Chaotic Dynamical System and SHA-512	International Journal of Wavelets, Multiresolution and Information Processing	SCIE	https://doi.org/10.1142/S0219691320500423	2020	0.56
5	Frederick Swartz D Daniel, Mohamed KA Junaid, B Jaison, Anita JT Rose	Dynamic association and participant based adaptive streaming in small base station for live video conference on 5G networks	Transactions On Emerging Telecommunications Technologies	SCIE	Vol 29 Issue 5	2018	1.594
6	K.Anitha B.Jaison	A Novel Enriched LASSO Based Compression Technique for Energy Efficient Wireless Sensor Networks	Advances in Systems Science and Applications	Scopus	Vol 20, No.1 ISSN (Online) 1078-6236	02020	0.51
7	Shaik Hedayath Basha, Jaison B	A Novel Secure Message ransmission using Elliptic Curve Diffie Hellman Key Exchange protocol	International Journal of Scientific and Technology Research	Scopus	E-ISSN:2277-8616, VOLUME 9, ISSUE 02	20	0.32
8	Dr.B.Jaison	Tamil text detection in	International	Scopus	ISSN: 2249	19	

		videos using Gradient Vector Flow and Fuzzy C-Means	Journal of Engineering and Advanced Technology (IJEAT)		– 8958, Volume-9 Issue-2		
9	Dr.B.Jaison	Design and implementation of sequential circuit based on low power using 45nm technology	International Journal of Recent Technology and Engineering	Copernicus, Google Scholar, Cross Ref	ISSN 2277-3878 Vol 7, Issue 6S3	19	
10	Dr.B.Jaison	Block chain based certificate Issuing and validation	International Research journal of Engineering and Technology	Copernicus, Google Scholar, DRJI	ISSN: 2395-0072	19	
11	Dr.B.Jaison	Data transmission for proximity devices using ultrasonicsound waves	International Research journal of Engineering and Technology	Copernicus, Google Scholar,	ISSN: 2395-0072 Vol 6, Issue 3	19	
12	Dr.B.Jaison	Design and implementation of sequential circuit based on low power using 45nm technology	International Journal of Recent Technology and Engineering	ISSN 2277-3878 Vol 7, Issue 6S3	Scopus Indexed	2019	
13	Dr.B.Jaison	Block chain based certificate Issuing and validation	International Research journal of Engineering and Technology	ISSN: 2395-0072	Copernicus, Google Scholar, DRJI	2019	
14	Dr.B.Jaison	Data transmission for proximity devices using ultrasonic sound waves	International Research journal of Engineering and Technology	ISSN: 2395-0072 Vol 6, Issue 3	Copernicus, Google Scholar, DRJI	2019	
15	Dr.B.Jaison	Investigation on Low Power for Reducing Counter Delay Digital Circuit Using 45nm Technology	International Journal of Engineering & Technology,	7 (4.6) (2018) 583-585	Scopus Indexed	2018	
16	Dr.B.Jaison	An Overview of Data Mining Techniques for Maize Yield	International Journal of Engineering &	7 (4.6) (2018) 490-	Scopus Indexed	2018	

		Prediction	Technology,	492			
17	Dr.B.Jaison	Plant Disease Identification using Image Classification Techniques	International Journal of Engineering Science and Computing	Vol 8 Issue 4, ISSN:2321 3361	Google Scholar	2018	
18	Dr.B.Jaison	A Survey: Detailed Study on Various attacks and Remedies of WSN	International journal of Pure and Applied Mathematics	Volume 119 No. 12 2018, 16679-16697	Scopus Indexed	2018	
19	Dr.B.Jaison	Design of an Efficient Multiplier Implemented in Ancient Vedic Math Approach for high speed digital circuits	International journal of Pure and Applied Mathematics	Volume 119 No. 15, 2018, 279-284	Scopus Indexed	2018	
20	Dr.B.Jaison	An ID Based Aggregate Scheme for Multiuser Broadcast Authentication in Wireless Sensor Networks	IJSRD-International Journal for Scientific Research & Development|	Vol.6, Issue 02,2018 ISSN2321-0613	Google scholar, Scribd, Academia.edu	2018	
21	Dr.B.Jaison	Design and analysis of 7T SRAM using Nano scale technology	International journal of Pure and Applied Mathematics	Volume 118 No. 20 2018, 3471-3475	Scopus Indexed	2018	
22	Dr.B.Jaison	Design of systematic retroverted multiplier for low-power desolation	International journal of pure and Applied Mathematics	Volume 118 No. 20 2018, 3431-3438	Scopus Indexed	2018	
23	Dr.B.Jaison	Smart Charger for Mobile phones using Embedded System	International Journal of Scientific Research in Computer Science, Engineering and IT	IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307	Google scholar. DOAJ, Web of Science	2018	
24	Dr.B.Jaison	Survey on patended and un patended video water marking	International Conference on advanced	Volume 118 No. 20	Google scholar	2017	

		techniques	computing and communication systems	2018, 3471-3475			
25	Dr.B.Jaison	Design of SRAM Architecture With Low Power Without Affecting Speed Using Finfet	International Journal On Smart Sensing And Intelligent Systems	Volume 6, Issue 2, ISSN Online : 2277-5420	Scopus Indexed, DOAJ , EBSCO	2017	
26	Dr.B.Jaison	Detection of type of Flight using Image Processing Techniques	Indian Technology Congress held at Bangalore	Volume 119 No. 12 16679-16697	Google scholar	2017	
27	Dr.B.Jaison	Design of serial full adder using Finfet logic	Fronteiras journal of social,Technological and Environmental Science	Vol.6 ISSN2238-8869 PP.60-67	Scopus Indexed, DOAJ	2017	
28	Dr.B.Jaison	A review of stability aware clustering algorithm in vehicular adhoc network	Pakistan journal of Biotechnology	Vol.14, Sp.Issue II pp-1-5	Scopus Indexed	2017	
29	Dr.B.Jaison	Design Of SRAM Architecture With Low Power Without Affecting spped based on shorted gate (SG) mode using Finfet	International journal of pure and applied mathematics	Issn 1311-8080 Pp:305-310 Vol.115, No.7	Google Scholar, CrossRef	2017	
30	Dr.B.Jaison	A scalable secure file sharing system for dynamic groups in cloud computing	International journal of Computer Science and Network	Volume 6, Issue 2, ISSN (Online) : 2277-5420	CiteSeer, Google Scholar	2017	
31	Dr.B.Jaison	Hybrid classification techniques for microarray data	National Academy Science Letters	volume 38, Issue 5, 0250-501x	Scopus, SCI Indexed	2015	1.20
32	Dr.B.Jaison	A Hybrid approach for gene selection and classification using support vector machine	The International Arab journalofInformation Technology	Vol.12, No.6A	Elesiver, Thomson ReutersEBSCO, DOAJ	2015	0.78
33	Dr.B.Jaison	Cluster based approach for efficient features is	International Journal of	Vol.10, No.20,	Scopus(2010-2017),	2015	

		subset selection using kruskals algorithm for microarray data	applied engineering Research	ISSN:0973-4562	EBSCOhost, Google Scholar,		
34	Dr.B.Jaison	A discrete wavelet based features extraction and hybrid classification technique for microarray dat and analysis	The Scientific World Journal	Volume 119 No. 12 , 16679-16697	Scopus	2014	

Signature of Head of the Institution /Industry
(Name with seal)

Computer Communications 152 (2020) 316–322

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms

P.P. Devi [a,*], B. Jaison [b]

[a] Aalim Muhammed Salegh College of Engineering, India
[b] R.M.K Engineering College, India

ARTICLE INFO

Keywords:
Clone attack
Performance analysis
Hybrid clone node detection
Key distribution
Wireless sensor network
SDN
QoS

ABSTRACT

WSN is an infrastructure less network that consists of mobile nodes that communicate with each other over wireless links. WSN is vulnerable to the node replication attack (clone attack). Attackers through compromising one sensor node replicate many clones having the same identity (ID) from the compromised node, and place these clones in various places of network. Clones contain all the credentials of legitimate member so appears authentic. This makes the conventional cryptographic tools useless and clone detection difficult. Once the node replication attack has been successful it can help the attacker to exploit almost all of the network operations, like routing, data collection, and key distribution, and also to help launch various other attacks such as black hole, wormhole etc. This proposed work therefore attempts a SDN based mechanism that implements a network level route analysis and time-based analysis methods which involves a low cost timely monitoring of the environment to identify and avoid redundant nodes which may be caused due to cloning attack. Thus, the SDN based cyber security applications are most useful in this situation. The implementation of this SDN based mechanism in WSN helps in maintaining and improving the QoS (Quality of service) constraints. The hybrid clone node detection (HCND) mechanism helps to detect the clone node present in the wireless network. This is to perform efficient clone detection in such a way to eliminate cloning attack in proactive fashion. To detect clones locally as well as across geographical region through cost effective identity verification procedure. This method helps to protect the wireless sensor network from the node identity replicas using the superimposed SDIS junction code. The node identity replicas help to choose the credible path for successful transmissions. The superimposed method is to be used for retrieval of information from node participating on the network. To thwart cluster of attacks hosted from the clones, by removing the hosting clones. The simulation result shows that there is the performance analysis of various parameters such as false positive, false negative ratio analysis, precision analysis, recall analysis and detection analysis.

1. Introduction

The wireless sensor network is defined as a network of devices which is to communicate the details gathered from a monitored field with a way of wireless links. The information is to be forwarded through multiple nodes within the gateway. This data is to be connected to other networks like wireless Ethernet. It consists of base stations and various numbers of nodes. This network is to be used to diagnose physical or environment conditions such as sound, pressure, temperature and co operatively which is pass information through the network to a main location. In the radio communication networks, the wireless sensor network has the various number structures with various topologies. In the wireless sensor network, there are various attacks are to be presented according to the different criteria such as domain of the attackers or the techniques which are to be used in attacks. There are two major categories are to be classified which are according the interruption of communication like passive attacks and active attacks. For this, software defined network is an efficient one for enhancing security against attack by maintaining QoS.

1.1. Clone Attack

The wireless sensor network is most vulnerable which the severe attack that is clone attack is. This method helps to detect the clone attacks which are present in the wireless sensor networks. There are various centralized and distributed techniques such as on the detection of clones in sensor networks using random key pre distribution, detecting node clones in sensor networks, real time detection of clone attacks in wireless sensor network, hierarchical node replication attacks detection in wireless sensor network, compressed sensing based clone identification in the sensor networks, fast detection of replica node

* Corresponding author.
E-mail addresses: devisayz@gmail.com (P.P. Devi), bjn.cse@rmkec.ac.in (B. Jaison).

https://doi.org/10.1016/j.comcom.2020.01.064
Received 25 September 2019; Received in revised form 23 December 2019; Accepted 27 January 2020
Available online xxxx

Lemuria: A Novel Future Crop Prediction Algorithm Using Data Mining

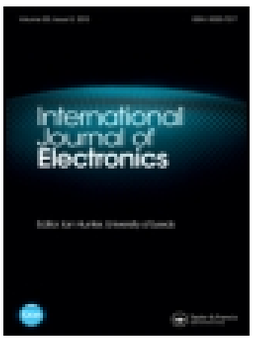
M Tamil Selvi ✉, B Jaison

The Computer Journal, bxaa093,
https://doi.org/10.1093/comjnl/bxaa093
Published: 30 July 2020 **Article history** ▾

Abstract

Agriculture exhibitions an important role in the progression and enlargement of the economy of any country. Prediction of crop yield will be useful for farmers, but it is difficult to predict crop yield because of the climatic factors such as rainfall, soil factors and so on. To tackle these issues, we are implementing a novel algorithm called Lemuria by applying data mining in agriculture especially for crop yield analysis and prediction. This novel algorithm is the hybridization of classifiers for pre-training, training and testing: deep belief network for feature learning, *k*-means clustering together with particle swarm optimization (PSO) to get the global solution as well as naïve Bayes clustering with PSO for testing. The performance of the Lemuria algorithm is evaluated in Python, which provides an accuracy of 97.74% for crop prediction by considering the rainfall dataset and also stated that this gives the optimum results in comparison with the existing methodologies.

Issue Section: Original Article



International Journal of Electronics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tetn20

Design of low power 16-bit counter with Programmable Combinational Logic and Integrated Clock Gating using 16-nm technology

S Mohamed Sulaiman , B Jaison & M Anto Bennet

To cite this article: S Mohamed Sulaiman , B Jaison & M Anto Bennet (2020): Design of low power 16-bit counter with Programmable Combinational Logic and Integrated Clock Gating using 16-nm technology, International Journal of Electronics, DOI: 10.1080/00207217.2020.1793398

To link to this article: https://doi.org/10.1080/00207217.2020.1793398

Accepted author version posted online: 10 Jul 2020.
Published online: 23 Jul 2020.

INTERNATIONAL JOURNAL OF ELECTRONICS
https://doi.org/10.1080/00207217.2020.1793398

Taylor & Francis
Taylor & Francis Group

Design of low power 16-bit counter with Programmable Combinational Logic and Integrated Clock Gating using 16-nm technology

S Mohamed Sulaiman[a], B Jaison[b] and M Anto Bennet[c]

[a]ECE, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India; [b]CSE, RMK Engineering College, Chennai, TN, India; [c]ECE, Vel Tech

ABSTRACT

To demand high power back up by increasing the user's need for applications in a single IC, the power dissipation takes place. The proposed two approaches are control Logic (CL) with Integrated Clock Gating (ICG) and Programmable Combinational Logic(PCL) and Gate Logic(GL) with ICG to achieve the low power and low dynamic leakage in 16-bit Counter. These approaches operate in different Logic to Generate/stop the clock for low-power digital circuits. The First approach of control Logic with ICG stops the clock only for single Most Significant Flip Flop Transistor. This approach consumes 1.6 mW and 15% more power savings than Existing. But the second approach only consumes 0.0261 mW power, which is 98% more power savings than a first proposed approach of CL with ICG and conventional counters. These dramatic boom power savings by stopping the clock for all redundant transition in Most Significant Flip Flop Transistors using PCL & GL with ICG. Analyse the second approach without ICG for 16-bit counter will consume 0.0334 mW, which consumes 21.96% high power than the presence of ICG in counter circuits. Moreover, the same proposed technique of the second approach applies for ISCAS'89 S444 circuits, which saves >90% power improvement than the conventional method and ordinary 16-bit counter-power analysis by the same technology, which consumes 42.42% high power than proposed low-power counter. The Low Power 16-bit counter design implementation using 16 nm Cadence Genustechnology, which attains the dynamic leakage with ICG is 0.170nW and without ICG is 0.177nW with an operating voltage of 0.8 V.

ARTICLE HISTORY
Received 3 June 2019
Accepted 3 May 2020

KEYWORDS
Programmable Combinational Logic (PCL); Control Logic (CL); Gate Logic (GL); Integrated Clock Gating(ICG); low power; redundant switching transition; 16-bit counter; 16 nm technology

I. Introduction

Dynamic power is devoured (Kim et al., 2009) (Peddersen & Parameswaran, 2007) overall components of a chip. The clock arranges is one of the vast consuming dynamic power. The half of dynamic power is disseminated in the clock organise (Hwang & Lin, 2012) (Neil, 2006). The dynamic exchanging power scattering turns into the most conspicuous segment for power utilisation in VLSI circuits. Another normal technique is control gating to diminish the power without influencing the speed of the circuit (Basireddy et al., 2019) (Moss et al., 2019).

CONTACT S Mohamed Sulaiman sulaimanmtech@gmail.com ECE, Vel Tech High Tech Dr.Rangarajan Dr. Sakunthala Engineering College, Chennai 600062, Tamil nadu, India

International Journal of Wavelets, Multiresoultion and Information Processing

World Scientific
www.worldscientific.com

An Efficient Novel Color Image Encryption Algorithm based on 3D Lü Chaotic Dynamical System and SHA-512

K. Sundara Krishnan

Department of Computer Science and Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi, Tamilnadu, India
sundarakrishnank@gmail.com

B. Jaison

Department of Computer Science and Engineering, RMK Engineering College, Chennai, Tamilnadu, India
bjn.cse@rmkec.ac.in

S.P. Raja

Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India
avemariaraja@gmail.com

In this paper, an efficient novel dual permutation-substitution structure based color image encryption algorithm is proposed. Initially, the Secure Hash Algorithm-512 (SHA-512) is applied to the input image to generate the initial values for the Lü system dynamically. In the first stage of permutation, inter-color-component pixel shuffling is carried out with a circular swapping mechanism. In the second stage, intra-color-component pixel shuffling is executed, based on pseudorandom positions generated by the Lü chaotic system. Pixel values are changed in the substitution stage, based on float-valued chaotic sequences generated by the Lü system. The performance of the proposed algorithm is evaluated with metrics such as key space, key sensitivity, histograms, correlation coefficients (vertical, horizontal and diagonal), information entropy, number of pixel change rates (NPCR), unified average changing intensity (UACI), peak signal-to-noise ratio (PSNR), mean absolute error (MAE), contrast analysis, encryption time, and the National Institute of Standards and Technology Special Publication 800-22 Statistical Test (NIST SP 800-22). The experimental results obtained and performance assessment show that the proposed scheme has produced good results.

Keywords: Image encryption; Chaos; Lü system; Permutation; Substitution

1. Introduction

Images are a primary source of information in disciplines such as medical imaging, defense communication, remote sensing and personal lives. Remarkable advancements in communication technology and an escalation in the use of social media and assorted multimedia applications have culminated in the transmission of masses of digital image data over the unsecure public Internet. Images often contain confidential and sensitive information. As a consequence, secure image transmission is inevitable, and image encryption is the best way to ensure its security. Contrasted with text data, images are usually larger in size and have a high correlation among pixels, thus permitting data loss. Owing to this distinctive nature of images, conventional ciphers such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) are poorly suited to image encryption[23, 27]. Chaos and

Received: 9 October 2017 | Revised: 15 January 2018 | Accepted: 15 February 2018

DOI: 10.1002/ett.3300

RESEARCH ARTICLE

WILEY

Dynamic association and participant based adaptive streaming in small base station for live video conference on 5G networks

Frederick Swartz Daniel D | Mohamed Junaid K.A | Jaison B | Anita Rose J.T

R.M.K. Engineering College, Chennai, India

Correspondence
Frederick Swartz Daniel D, R.M.K. Engineering College, Chennai, India.
Email: frederick.me@gmail.com; dfrederick75@yahoo.co.in

Abstract

Targeting to handle the explosive growth of mobile media streaming, the emerging fifth-generation systems need to manage control plane and data plane appropriately. The control plane is used for node association in the heterogeneous cellular network and data plane for media streaming with heterogeneous user equipment. To satisfy the aforementioned requirements, we proposed a solution to alter the control plane and data plane by systematic usage of in-network resource available in wireless edge (eg, macro, pico, and femto) small base stations (SBSs) for the deployment of smart association policies and media processing technique that improve the efficiency in fifth-generation wireless networks. On the other hand, due to the broadcast nature of wireless medium, we introduce the media processing agent (MPA) that would reside in SBSs to process the media on the fly and then deliver streams adaptively to the participants. MPA can identify the presenter among the participant to create the server channel with media server and the observer can service from MPA itself. To better exploit the participant's node association with the nearby SBSs, association policies are enhanced with concerns on dynamic association with SBSs. In addition, we describe a heuristic algorithm that provides significant performance gains compared with the existing centralized processing schemes. Numerical results are presented with realistic parameters for the media processing speed, and the quality of delivery demonstrate up to 20% reduction in central processing unit usage over existing (centralized) media processing schemes.

1 | INTRODUCTION

An extraordinary worldwide growth of mobile data traffic in cellular networks today is video streaming. Observing evidence suggests that video-based communication will keep increasing its share of the cellular traffic at an even faster pace. The reason behind this phenomenon is the explosive demand for high-quality video streaming from mobile devices (eg, tablets and smartphones). These expansions place huge pressure to mobile network operator (MNO) who need to advance the technologies and develop a video delivery solution to offer higher data rates that can keep up with this demand for high-quality video. Fifth generation (5G) is the next-generation heterogeneous cellular networks (HCNs) and multitier architecture that envisage to deliver orders of magnitude higher throughput, lower delay, and energy efficiency. HCNs introduce low-power small base station (SBS) that form around them picocells and femtocells respectively.[1] The novel

*Adv Syst Sci Appl 2020; **01**; 66-82*
Published online at http://ijassa.ipu.ru/index.php/ijassa/article/view/803

A Novel Enriched LASSO Based Compression Technique for Energy Efficient Wireless Sensor Networks

Anitha K[1], Jaison B[2], Nalini M[3], Shiny Irene D[4]

[1)] *Department of Computer Science and Engineering, Saveetha School Engneering, Chennai, India*

Email: anithak.rameshr@gmail.com

[2)] *Department of Computer Science and Engineering, R.M.K Engineering College, Chennai, India*

Email: bjn.cse@rmkec.ac.in

[3)] *Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai, India*

Email: nalinitptwin@gmail.com

[4)] *Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai, India*

Email: dshinyirene@gmail.com

Abstract: The capability of transmission in Wireless sensor networks (WSN) is circumscribed due to the precincts in energy utilization, controlled resources of transmission devices and network components. Information compression is taken into account as the best option, because the major part of energy consumed is for transmission of information. Habitually Lossy compression is adopted, since WSN abides some error in the reconstructed signals subjected to some acceptable tolerance. Lasso based models have been ascertained their capability to effectually compress both multivariate and univariate data. Traditional Lasso considers ℓ1-norm regularization for learning in multi-dimensional data sets and assumes sparsity as model parameters. Lasso prominence on sparsity and deal with the correlation between the data points. However, model sparsity may be constricting and not essentially the foremost applicable assumption in several problem domains. To eliminate this limitation, an enriched lasso (MLasso) is proposed for compression bearing in mind both sparsity and correlation. In specific the strategy can select data that are having strong features to reconstruct the data and are less correlated between each other. Furthermore, an efficient Alternating Direction Method of Multipliers (ADMM) is adopted to resolve the ensuing sparse non-convex optimization problem. Extensive experiments on diverse datasets provides the proof that MLasso outperforms other similar algorithms for signal compression. Thus the proposed method ensures less energy consumption, decreases power loss and improves the operational life and reliability of network components.

Keywords: Multidimensional data, compression, energy efficiency, senor networks, lossy compression

1. INTRODUCTION

In current scenario, there is an immense development in usage of mobile technologies and remote sensing devices. Progresses in compact hardware and sensing devices aided to impart them into every object leading to Internet of Things (IoT) [1]. Large scale wireless sensor networks (WSNs) are employed to acquire and collect the data from different envi-

A Novel Secure Message Transmission using Elliptic Curve Diffie Hellman Key Exchange Protocol

Shaik Hedayath Basha, Jaison B

REF. NO: IJSTR-1219-26794

Abstract— The main objective of the proposed work is to develop a new simple method to secure the text messages in the transmission systems. ELLIPTIC CURVE DIFFIE HELMAN (ECDH) key exchange protocol is adopted which is one of the highly secure cryptography technique compared with other cryptographic techniques. In the proposed work prime elliptic curve is used to encrypt the input message signal. In the first step, a new convolution wheel is developed to convert the text message into modified ASCII value. Using these values and the elliptic prime curves the message is encrypted at the transmitter section, the channel is considered as a lossless noisy channel and the basic attacks like cipher text attack, cipher text only attack and chosen key attack were analyzed. It is found that the cipher text is very robust to various attacks and the probability that the attacker decrypt is very less. The cipher text is decrypted with the private key at the receiver end.

Index Terms— Attacks, Convolution Wheel, Decryption, ECDH, Encryption, Modified ASCII, Secure.

1 INTRODUCTION

IN the elliptic crypto system there are three schemes to solve the crypto problems they are integer factorization, discrete logarithm and elliptic curve discrete logarithm problem. In the public cryptography system a key pair is selected so that the problem of deriving the sender's private key from the corresponding public key is equivalent to solving a computational problem that is believed to be intractable. The elliptic curve cryptography problem can be done in the four different methods they are EC over real numbers, EC over complex numbers, EC over prime curves (Zp) and EC over Galois field or finite fields (F_{2^m}).

1.1 General Elliptic Curve over a real number field 'F':

Over a real number field, let a_1, a_2, a_3, a_4 and a_6 are the variables defined in the elliptic curve (E) it is defined as

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Δ is the discriminant of E, it is defined as the following and $\Delta \neq 0$.

$$\Delta = -d_2^2d_8 - 8d_3^4 - 27d_6^2 + 9d_2d_4d_6 \quad (2)$$

$$d_2 = a_1^2 + 4a_2 \quad (3)$$

$$d_4 = 2a_4 + a_1a_3 \quad (4)$$

$$d_6 = a_3^2 + 4a_6 \quad (5)$$

$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \quad (6)$$

If L is rational point on E, then

$$E(L) = \{(x, y) \in L\ X\ L: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \quad (7)$$

where ∞ is point at infinity.

1.2 Elliptic curve over real numbers(R) is simplified as

$$E/\boldsymbol{R} = y^2 = x^3 + ax + b; a, b \in \boldsymbol{R} \quad (8)$$

$$\text{Where } \Delta = 4a^3 + 27b^2 \neq 0 \quad (9)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2)$ and if $P \neq Q$ then, the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

if $P = Q$ then the third point is obtained by point doubling i.e. $P + Q = P + P = 2P$

$$x_3 = \lambda^2 - x_1 - x_2 \quad (10)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (11)$$

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}; if\ P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1};\ if\ P = Q \end{cases} \quad (12)$$

1.3 Elliptic curve over Prime field (Zp) is defined as

$$E/\boldsymbol{Z_p} = y^2 mod\ p = x^3 + ax + b\ mod\ p \quad (13)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2) \in \mathbf{Z_p}$ and if $P \neq Q$ then the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

If $P = Q$ then the third point is obtained by point doubling i.e. $P + Q = P + P = 2P$

$$x_3 = \lambda^2 - x_1 - x_2\ mod\ p \quad (14)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p \quad (15)$$

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}; if\ P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1};\ if\ P = Q \end{cases} \quad (16)$$

1.4 Elliptic curve over Galois field or finite fields ($\mathbf{F_{2^m}}$) is defined as

$$E/\boldsymbol{F}_{2^m} = y^2 + cy = x^3 + ax + b \quad (17)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2) \in \boldsymbol{F}_{2^m}$ and if $P \neq Q$ then the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 \quad (18)$$

- ***Shaik Hedayath Basha*** *is currently working as Assistant Professor in the Department of Electronics and Communication Engineering at RMK College of Engineering and Technology and pursuing Doctor in Philosophy degree in Information and Communication Engineering at Anna University, Chennai, India, PH-09104467900679. E-mail: shaikhedayathbasha@rmkcet.ac.in*
- ***Dr. Jaison B*** *is currently working as Associate Professor in the Department of Computer Science and Engineering at RMK Engineering College affiliated to Anna University, Chennai, India, PH-09104467906790. E-mail: bjn.cse@rmkec.ac.in*

Tamil text detection in videos using Gradient Vector Flow and Fuzzy C-Means

J.T.Anita Rose, B.Jaison, S.V.S.Harshavardhan, B.Krishna Teja, J.Dinesh Sai

Abstract: -In videos, detecting text with multifaceted scenarios is perplexing. Texts in those videos have content full data facts that will be applied for various applications. Here, a system is proposed to enrich the text detection process from video. Here, a new method is implemented that detects Tamil text based on Gradient Vector Flow (GVF) and fuzzy c-means. First the video is split into number of frames. To circumvent temporal redundancy in each frame, a key frame is chosen and the frame where the text be located is identified to be the key frame. The dominant edge pixel is identified in that frame by the sobel edge map. Edge components are detected conforming towards the dominant pixel in sobel detector for constructing Text Candidates (TC).Clustering of a pixel is performed to detect text by using fuzzy c means clustering algorithm. Finally text is detected.

Keywords : Gradient vector flow, Dominant pixel, Text candidate, Fuzzy C-means.

I. INTRODUCTION

Text entrenched in videos encompasseshuge number of valuablecontent that are applied to many real time applications. The semantic content present in the video is an important and useful information to be required for the processing of many real world applications [8,12,25]. Caption text and Graphics text – these are the different kinds of text available while processing with the text present in the video.

Scene texts are those texts that exist in the scenario of shooting the video. The scene text may be for example, the number present on the t-shirt of a football player, the name board of a shop, the license plate details of a vehicle. Scene text is also called graphics text. The Caption text is manually superimposed over the captured video to enhance the meaning of video/image. It is also called superimposed text. Plenty of methods exist for the purpose of extracting the useful information present in images throughout the past decade. This technique includes methods that deal with the texture properties of the image [5], small components of text combined to create words of text [11], edge identifying frameworks [12] and gradient based approaches [21]. Texture based methods extricate text regions along thecontextualcontent [13,16,26].

The approaches in connected component employ the principle of connecting small set of components to form text candidate regions [17, 23]. The approaches employed in edge based apply the principle of finding the boundaries of the image [1, 15, and 24].

The connected component method does not produce good results for images on multifarious backdrop of the image. The texture based methods works superior for multifaceted contextual content in videos compared to connected component approaches. The mixture of edge based method along with gradient feature based method performs better and becomes less apparent in processing of text detection of Tamil language for many reasons. The works in [22] and [28] primarily focuses on Multi-oriented text. In [20] a method based on laplacian was introduced to deal with the multi-oriented text. Our previous work on text detection is in [30, 31, 32, and 33]. As a result, a new-fangled way of methods is the need of the hour to detect Tamil text based on Gradient Vector Flow (GVF) and fuzzy c-means. This method will improve accuracy to detect Tamil text in videos.

II. PROPOSED METHOD

A new method is proposed that detects Tamil text based on Gradient Vector Flow (GVF) and fuzzy c-means. First the video is split into number of frames. To circumvent temporal redundancy in each frame, a key frame is chosen and the frame where the text be located is identified to be the key frame. The dominant edge pixel is identified in that frame by the sobel edge map. Edge components are detected conforming towards the dominant pixel in sobel detector for constructing text Candidates (TC).Clustering of a pixel is performed to detect text by using fuzzy c means clustering algorithm. Finally text is detected.

The Tamil language has different orientation comparable to English language. To tackle Tamil language text, we propose a novel method go detect dominant pixel by using GVF and Fuzzy C-means approach is employed for cluster formation on the pixels and thereafter the process of extracting useful text .

1) *Splitting of frames and key frame selection:*

The video which contains Tamil text is split into number of frames. To circumvent temporal redundancy in each frame, a key frame is chosen and the frame where the text be located is identified to be the key frame. Figure 1(a) shows the splitting of frames, the results of figure 1 (a) shows that the frame rate is considerably reduced which is the principal cause for the occurrence of temporal redundancy.

Revised Manuscript Received on December, 30 2019.

***** Correspondence Author

Dr. J.T.Anita Rose*, Associate Professor, Department of CSE, St.Joseph's College of Engineering, Tamil Nadu, India. Email: anitaswartz14@gmail.com

Dr.B.Jaison, Associate Professor, Department of CSE, R.M.K Engineering College, Kavaraipettai, Tamil Nadu, India. Email: bjn.cse@rmkec.ac.in

S.V.S.Harshavardhan, Student, IV Year CSE, Department of CSE, R.M.K Engineering College, Kavaraipettai, Tamil Nadu, India. Email: harshavardhan1234567891@gmail.com

B.Krishna Teja, Student, IV Year CSE, Department of CSE, R.M.K Engineering College, Kavaraipettai, Tamil Nadu, India.

J.Dinesh Sai Student, IV Year CSE, Department of CSE, R.M.K Engineering College, Kavaraipettai, Tamil Nadu, India. Email: j.dineshsai8358@gmail.com