Face Geometry and Handwritten Characters Based Biometric Text Steganography

Indradip Banerjee
Computer Science & Engineering Department, University Institute of Technology, The University of Burdwan
Burdwan, India.
ibanerjee2001@gmail.com

Kaustav Bandyopadhyay
Computer Science & Engineering Department, Seacom Engineering College
Howrah, India
banerjeekaustav11@gmail.com

Tarik A. Rashid
Computer Science and Engineering Department, University of Kurdistan
Hewler, Erbil 44001, KRG, Iraq
tarik.ahmed@ukh.edu.krd

Anand Mohan
Department of Physics L.N Mithila University
Darbhanga, Bihar, India
anandmohanjrf@gmail.com

Abeer Alsadoon
School of Computing and Mathematics, Charles Sturt University
Sydney, Australia
alsadoon.abeer@gmail.com

Ashok Kumar
M.L.S.M College, LN Mithila University
Darbhanga, Bihar, India.
prof.ashokkumar@rediffmail.com

2021 IEEE Bombay Section Signature Conference (IBSSC) | 978-1-6654-1758-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/IBSSC53889.2021.9673264

***Abstract*— Contemporary advancement in technologies has the responsibilities in the context of transmission, reproduction and manipulation of information. Thus an important protagonist formed by the fragment of information security vital. One of the information security contrivances in this literature is biometric information security. Steganography is an excellent prerogative for information diffusion over every public media by hiding the message. A new work in the literature of security has been proven with the help of handwritten atmosphere based text steganography algorithm and biometric based security. The biometric has been embedded to the text domain. The handwritten text based steganography procedure has been designed which can work in different Indian regional languages. Here the quantum approach has been assimilates before embedding and Revised SSCE code (Revised SSCE – Revised Secret Steganography Code for Embedding) used for enhancing the security.**

Keywords*— *Text Steganography, Numeric Handwriting, Security and Face Geometry.

I. INTRODUCTION

Announcement of the term “Security” is well known to each one from prehistoric age and hence the concept of information hiding has been launched. The topics “Information Hiding” is stands for hide features from a contents and that hidden part can be reachable to authentic user exclusively. This literature consists of various classifications. One of the most imperative classifications is steganography [1] which is derived from a work by Johannes Trithemus (1462-1516) entitled "Steganographia" and comes from the Greek language “στεγανό-ς γραφ-ειν” defined as "covered writing". It is the way of hiding evidence of the information in a cover so that is not suspicious for an eavesdropper. Steganography deviates from cryptography, steganography efforts to secret the presence of a message in the cover [2]. Steganography literature developed with the help of images, videoed, text, music etc. Steganalysis [3] is a reverse experiment to detect the existence. Below figure (Fig. 1) describes the types of steganography. Steganography have

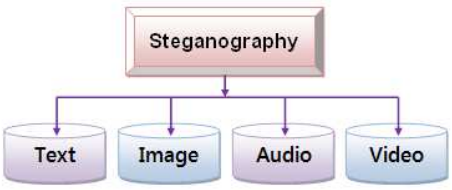

Fig. 1. Types of Steganography.

various techniques like Image, Audio, Video, Text etc. Text Steganography have various categories [4] like Format related, random generation, statistical, Linguistic and some technique on Quantum Approach [5].

Automatic recognition system of a creature derivative from the physiological and behavioural [6-11] characteristic is describing the Biometric security system. The word "biometrics" is a Greek word which plagiaristic from bio i.e. “life” and metric which means “to measure”. Biometric mechanism is that which can determine by the person's identity with the help of some pattern analysis of specific human attributes [7-8]. Biometric authentication organisms established on sensibility that involve ear shape, retina, hand geometry, fingerprints, hand vein, iris, and facial recognition systems. These features are characteristically inflexible imperfect of causing annoyance to human being. Conversely, behavioural biometric characteristics are shortly steady over a period of time. Some behavioral biometric systems includes dynamic keystroke, voice, verify of signs and analysis of gait.

II. BACKGROUND WORK

A. Steganography through Quantum way

This field explores very diminutive research work in steganography. Error syndromes based secret messages hiding mechanism [12] was hosted by Julio Gea-Banacloche. Technique Super Dense Coding modification has been developed by Natori et.al. which springs a modest behavior of quantum steganography [13]. Quantum based steganography concept has been hosted by Martin et.al. and this mechanism has been implemented by Bennett and Brassard's [14]. Three different quantum steganography protocols has been developed by Curty e.al. in [15].

B. Quantum gate

Quantum gate embed 2^h x 2^h unitary matrix, where *h is* qubits. This gate has same number of inputs and outputs. Quantum gates can be represented by qubit. Contributors has been used the Controlled gates as qubits to control the operations.

C. RCL (Reversible Classical Logic)

The concept of logical reversibility is to reconstruct input from output. The ir-reversible gate is NAND, it has one output and two inputs, while NOT is reversible. Table II shows Controlled-NOT (Con-NOT) which performs a NOT

978-1-6654-1758-7/21/$31.00 ©2021 IEEE

(shoes in Table I) on the second bit if the first bit is$\langle 1\rangle$, but or else has no effect.

TABLE I. NOT - TRUTH TABLE

NOT	<0>	<1>
<0>	0	1
<1>	1	0

TABLE II. C-NOT - TRUTH TABLE

C-NOT	<00>	<01>	<10>	<11>
<00>	1	0	0	0
<01>	0	1	0	0
<10>	0	0	0	1
<11>	0	0	1	0

The proof of the Con-NOT is given below [16]:

Let $\left\{|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}\right\}$ be the orthonormal basis.

Let, $|\psi\rangle=x|0\rangle+y|1\rangle=\begin{bmatrix}x\\y\end{bmatrix}$ and $|\phi\rangle=y|0\rangle+x|1\rangle=\begin{bmatrix}y\\x\end{bmatrix}$. $|\phi\rangle$ be the flip qubit of $|\psi\rangle$. Recall that $|\alpha\rangle\otimes|\beta\rangle=|\alpha\rangle|\beta\rangle=|\alpha,\beta\rangle$ …(1)

i. In case of 0 Cont. qubit

Problem: $CNOT\ \ |0,\psi\rangle=|0,\psi\rangle$

Con-NOT dimension assumes as

$$|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},|01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},|10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},|11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

Then, confirm whether

$$|0,\psi\rangle=x|0\rangle|0\rangle+y|0\rangle|1\rangle=\begin{bmatrix}x\\y\\0\\0\end{bmatrix}\ldots.(2)$$

So

$$CNOT\ \ |0,\psi\rangle=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}x\\y\\0\\0\end{bmatrix}=\begin{bmatrix}x\\y\\0\\0\end{bmatrix}=|0,\psi\rangle \quad \ldots(3)$$

Hence Con-NOT doesn't change qubit $|\psi\rangle$, if first qubit = 0.

ii. In case of 1 Cont. qubit

Problem: $CNOT|1,\psi\rangle=|1,\phi\rangle$, Con-NOT gate flips qubit $|\psi\rangle$.

1st demonstration, $|1,\psi\rangle=\begin{bmatrix}0\\0\\x\\y\end{bmatrix}$.

$$CNOT\ \ |1,\psi\rangle=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}0\\0\\x\\y\end{bmatrix}=x\begin{bmatrix}0\\0\\0\\1\end{bmatrix}+y\begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad \ldots(4)$$

Consequently $|1,1\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$ and $|1,0\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$, using these on the above equation springs

$$CNOT\ \ |1,\psi\rangle=x|1,1\rangle+y|1,0\rangle=|1\rangle(x|1\rangle+y|0\rangle)=|1,\phi\rangle\cdots(5)$$

Consequently Con-NOT gate flips qubit $|\psi\rangle$ into $|\phi\rangle$ if the control qubit = 1. Now it has been observed that Con-NOT matrix is multiplied by a column vector, it also been noticed that the operation on the first bit is identity.

D. Steganography in the context of Text

Text in any languages is the media used form historical age in this writings. Before the electronic age the peoples uses telegrams, letters, paragraphs and books to hide secret information within their texts. The concept hiding of information in digital age is like before called as text steganography. It can be categorized by three different techniques like formatting oriented, statistical as well as random generation and linguistic way [17].

E. BIS (Biometric Information Security)

Physiological or behavioral attributes like face, fingerprint, iris, retina and DNA are the main features of BIS [18]. There are various ways found in biometric technique:

Fingerprint [19], is belongs to pattern recognition portion. Fingerprint ridges have patterns like Whorl, Loop and Arch. Examining the intricate construction of the layer of blood vessels [20] at retina is not utterly transmissibly resolute i.e. back of the eye side is elaborate and thus each person's retina is irreplaceable. Analyzing facial characteristics of a human is called face biometry [21]. Human hand shape is also a biometric authentication parameters that can analyzes as well as computed [22]. In case of nose biometric mechanism [23] the features extracting from the nose and various classification techniques have been worked out. Ear biometric security, it is also an interesting authentication method, through which human can identify by analyzing and measuring shape and area of an ear [24]. Signature is an important biometric authentication technique where writing speed, velocity and pressure of writing are used as features [25]. Iris [26] system is another biometric approach through which it can be analyzed features using mathematical function of pattern recognition by the dimension of the colored ring which is belongs to the pupil tissue of an eye. Voice biometrics [27] is another mechanism and it need not requires any new hardware. Vein structure visibility depends on diverse concerns alike age of skin, thickness, temperature, physical motion, skin veins depth. L. Wang et al. [28] developed an algorithm using the thermal image vein. Kumar et al. [29] developed a vein junction points authentication system.

F. Face Geometry

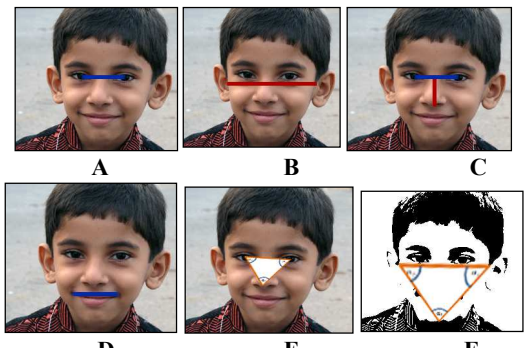

Fig. 2. Face Geometry Technique

The above described biometric methods are diverse because of contradictory approaches like performance of method, level of security, cost, etc. Among them a

physiological characteristics based appreciation system is Face geometry. The virtual position of nose, two eyes and mouth in human face is unique all. Calculate length, width, curvatures and location of face objects can separate creature. Figure 2.A shows the eyes distance. Figure 2.B extent the ears distance. Figure 2.C calculate distance from forehead to nose. Length and breadth of leap dignified in figure 2.D. Eyes and nose angles calculated in figure 2.E and ears and mouth in figure 2.F.

Contributors developed a new quantum supported handwritten text based biometric text steganography skill distant from the former techniques. In this contribution the authors proposed an algorithm which can use the face geometry biometric authentication and handwriting based text steganography technique. The quantum based technique is implemented in Text steganography domain which can work on different Indian regional languages in this work.

III. Proposed Methodology

Contributors contemporaneous a as well as Handwritten Characters and Face Geometry based Text steganography through quantum approach. This work exactly deals with text steganography practices with some of Indian regional languages like Bengali, Gujarati, Panjabi and Oriya etc. some Indian regional languages as the cover medium. Text based steganography process is to amend or alter the ASCII character of an existing text particularly in an explicit location. Contributors used MSG_{BIT} as parameters of face geometry. MSG_{BIT} is the secret message of digital character format and used as bit stream in the algorithm. After capturing the image through any capturing device the algorithm search out the face portion through existing mechanism. The algorithm can extract the above declared features of face and calculate distances from specific points of face. After that it measure the angles (α_1, α_2, α_3) as well from the virtual created triangle by the help of face bojects.
To create a secret message the system requires the combination of angles of α_1, α_2, α_3 and distance values. Then Revised SSCE code along with passkey has also been used to encrypt the secret message. Then use the handwritten Indian regional language text as cover. A matrix formed by message length and map C-NOT truth table. The mapping mechanism shown in table III. How to map the entire message shown in table IV. Replacing practice can unchanged the length of stego and cover. The reverse algorithm can get back the original information. The receiver authentication also processed by the help of α_1, α_2, α_3.

TABLE III. Quantum Truth Table Mapping

C-NOT	<00>	<01>	<10>	<11>
<00>	1	0	0	0
<01>	0	1	0	0
<10>	0	0	0	1
<11>	0	0	1	0

▮	32	118	69	117	69	120	79	106	115	65	32	66
164	▮	69	107	82	32	107	112	126	65	39	110	118
85	115	107	▮	77	67	69	85	32	93	97	166	32
118	110	▮	118	32	34	106	115	93	32	83	69	100
107	83	107	32	106	110	32	32	118	65	162	85	126
126	126	115	103	71	93	96	77	32	79	32	126	89
85	107	106	82	93	118	112	172	71	126	49	32	115
44	118	69	118	126	32	119	100	126	89	48	96	100
32	65	32	97	32	83	32	126	101	121	48	121	32
50	115	96	32	112	118	117	32	32	32	32	125	112
53	66	161	96	168	103	93	103	71	110	82	97	164
32	118	32	121	66	32	100	164	89	118	162	121	42
79	69	52	125	126	110	115	77	103	32	32	106	32
96	97	45	32	32	117	66	32	32	89	69	115	65
97	101	48	117	117	77	126	93	112	126	172	32	115
82	115	32	97	106	96	73	126	168	32	103	106	110
112	96	96	65	112	32	118	32	83	67	116	69	83
118	103	115	115	115	89	44	93	32	120	89	96	126
32	115	107	96	32	126	32	121	32	112	106	32	107
45	66	32	32	117	93	117	110	100	32	118	107	118

TABLE IV. Mapping Technique

Language	ASCII	Character	ASCII	Character		
BEAGALI	69	ক	34	‘	0	0
	69	ক	39	’	0	1
	77	ঝ	34	‘	1	0
	77	ঝ	39	’	1	1
GUJARATI	113	ક	34	‘	0	0
	113	ક	39	’	0	1
	173	ર	34	‘	1	0
	173	ર	39	’	1	1
PUNJABI	67	ਉ	34	‘	0	0
	67	ਉ	39	’	0	1
	65	ਆ	34	‘	1	0
	65	ਆ	39	’	1	1
ORIYA	107	ଲ	34	‘	0	0
	107	ଲ	39	’	0	1
	109	ଭ	34	‘	1	0
	109	ଭ	39	’	1	1

IV. ALGORITHMS

Different algorithm of a developed system are given:

A. *Encryption and Decryption*

- Input: Message and Passkey
- Pick character: ASCII of message.
- Change: ASCII code ->*SSCE*
- Add: Passkey -> Revised SSCE value.
- Regenerate.

B. *Embedding*

- Select: Message
- Encrypt: Through *SSCE value*
- Mapping: MATMSG (N x N) vertically or horizontally -> insert message by replacing ‘0’.
- Message sequence checking: MSG (Pick two bit sequence).
- Start from first: Cover text (TX).
- Checking: TX
- If Language is
  - Bengali : Map -> Bengali Character
  - Gujarati: Map -> Gujarati Character
  - Oriya: Map -> Oriya Character
  - Panjabi: Map -> Panjabi Character
- Repeat: Until end.

C. *Extracting*

- Select: MATMSG (N x N)
- Map quantum C-NOT: MATMSG (N x N) -> vertically or horizontally.
- Extract: Message (‘0’Th position of C-NOT).
- Select: Stego (TX)
- If Language is
  - Bengali: extract -> Bengali charater
  - Gujarati: extract -> Gujarati charater
  - Oriya: extract -> Oriya charater
  - Panjabi: extract -> Panjabi charater

D. *Authentication Algorithm*

- Capture: Images (IM_{IMAGE})
- Calculate threshold (T_{THRES}) : IM_{IMAGE}
- Transfer: IM_{IMAGE} -> Binary image (BIN_{IMAGE}) , T_{THRES} and detect-> face boundary.

- Detect center points: face (*F*), eyes (E) and nose (*N*) (*IM*$_{IMAGE}$)
- Measure distance
- Measure angle: *F*, *E*, *N* and store in the *MSG*.
- End

V. Mathematical Analysis

Encryption and Decryption: Row xth and column yth of a matrix is referred to as (x, y)th entry of a matrix **A.**

$A[x, y]$ or $a_{x,y}$. A = $[a_{x,y}]_{x=1,2,....,m \text{ and } y=1,2,....,n}$

Row - Column operation –

Row

1. R_x < —> R_y
2. $_sR_x$ —> R_y
3. $_sR_y$ —> R_x

Column

1. C_x < —> C_y
2. $_sC_x$ —> C_x
3. $_sC_y$ —> C_y

$A[x, y] \rightarrow A'[x, y]$

$A'[x, y] \rightarrow A'T[x, y]$.

Passkey P with $A'^T[x, y] \rightarrow P.\ A''^T[x,y]$.

VI. Results Analysis

To enter into the result portion the contributor shows some results in an Indian regional language. The system simulated the results are shown in the Fig. 3, 4 and 5.

જયપુર, તા. ૯, મે. આઈપીઓલ-૫ની પ૬મી ગેયસ અને યેનઈ સુપર કિંસ સામેની મેચ શરૂ થતાની સાથે જ વરસાદના વિઘ્ન સાચે આઈપીએલ-૫ની પ૬મી રાજસ્થાન રોયલ્સ અને પેન્નઈ સુપર કિંગ્સ સામેની મેચ શરૂ થતાની સાથે જ વરસાદના વિઘ્ન સાથે બંધ થવા પામી હતી. બીજે વરસાદ બંધ થતા મેચ ફરી

Fig. 3. Cover Text of developed algorithm

File Edit Format View Help

1010111010110010010010000111101010101010101010110100

Fig. 4. Secret Message of developed algorithm

જયપુર, તા. ૯, મે. આઈપીઓલ-૫ની પ૬મી ગેયસ અને યેનઈ સુપર કિંસ સામેની મેચ શરૂ થતાની સાથે જ વરસાદના વિઘ્ન સાચે આઈપીએલ-૫ની પ૬મી રાજસ્થાન રોયલ્સ અને પેન્નઈ સુપર કિંગ્સ સામેની મેચ શરૂ થતાની સાથે જ

Fig. 5. Stego Text of this algorithm

Similarity Measure:

Correlation used here to measure the similarity in between cover as well as stego.

n measurements of Pearson correlation *r* between *X* and *Y* shown as x_i and y_i (i = *1, 2, . . . n).*

Correlation coefficient $r_{xy} = \dfrac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{(n-1) S_x S_y}$ … (6)

where $\bar{x}$ and $\bar{y}$ are the sample means, S_x and S_y are the sample standard deviations of *X* and *Y*. The Correlation score of comparing cover and different stego of various length of message is furnished in Table V.

TABLE V. Correlation: Cover-Stego in Diffe. Message Length

MESSAGE LENGTH (In Character)	CORRELATION VALUE
10	0.991976
50	0.9987817621
100	0.9975177235
200	0.9951591513
300	0.9927451838
400	0.9903136183
500	0.9879305124
600	0.9855288135
700	0.9831311092
800	0.980737127
900	0.9783471344
1000	0.9759612819

After observing the Fig. 6 it can be proved that the cover as well as stego graphs are keep on identical. The Fig. 7 shows the input as well as output messages graphs, to view this graph in has been proved that they are similar and thus we can prove our method as well.

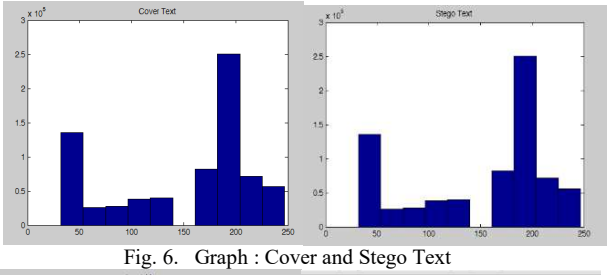

Fig. 6. Graph : Cover and Stego Text

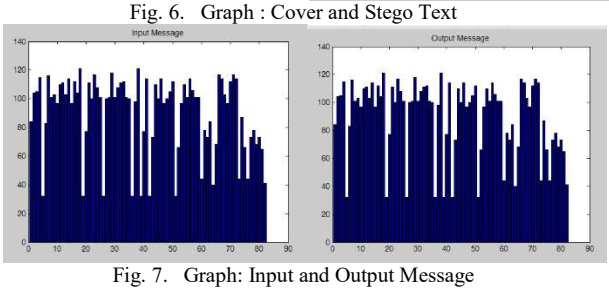

Fig. 7. Graph: Input and Output Message

Fig. 8 shows the GUI representation of proposed method.

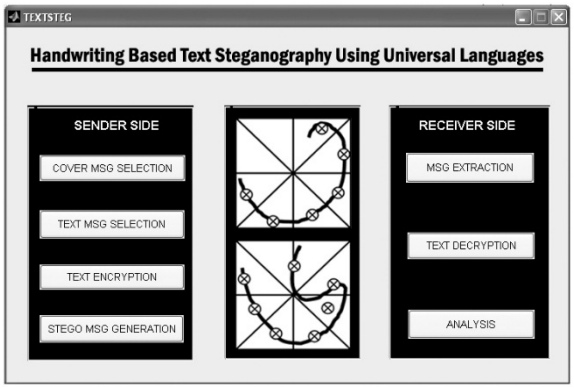

Fig. 8. GUI Representation

In Table VI the contributors have proved that the receiver side message generation system is faster comparatively sender side stego generation system.

TABLE VI. Computation Time of Stego & Message Generation

Message Length (Character)	Computation Time (in Second)		
	Stego Generation (A)	Message Generation (B)	Difference between (B-A)
10	0.1404009	0.1872012	0.0468003
50	0.6552042	0.6864044	0.0312002
100	1.2168078	1.3572087	0.1404009
200	1.9344124	3.0576196	1.1232072
300	2.7144174	3.3228213	0.6084039
400	3.5724229	4.3836281	0.8112052
500	4.5396291	5.616036	1.0764069
600	5.6940365	7.0512452	1.3572087
700	7.4256476	8.4864544	1.0608068
800	10.4208668	10.8576696	0.4368028
900	9.5784614	10.8888698	1.3104084
1000	9.3288598	11.4192732	2.0904134

Comparison of developed as well as previous existing some technologies are arguing in Table VII.

TABLE VII. COMPARISON WITH SUPPLEMENTARY EXPANSIONS

Existing Methods	Inter word and Inter paragraph Spacing Text Steganography [31]	Changing Words Spelling Text Steganography [30]	Letter Points and Extensions Text Steganography [32]	Author's Proposed Method
Details of the Method:	Lines or paragraph are vertically shifted. Information is hidden through an unique shape of the text.	Assigning the US words for hiding the bit 0 and UK words for bit 1.	Replacing the pointed and un pointed letter to 1 and 0 in Arabic language.	Universal language is used. Hand written letters to hold 00,01,10,11. Quantum approach is used to enhance security.
No of Embedding Bits:	Single (0 and 1)	Single (0 and 1)	Single (0 and 1)	Double (00,01,10,11)
Changes Occurred:	Lines, Word or Paragraph	Word	Letter	Letter pattern
Embedding Capacity:	Greater than Method 1 but lesser than Method 3, Method 5.	Lowest compared to other 4 methods.	Greater than Method 1 and Method 2 but lesser than Method 4 and Method 5.	Greater than all the previous method.
Similarity Measure:	Not Applicable	Not Applicable	Not Applicable	0.99

VII. Conclusions

This contribution is based on a novel area which explores the biometric security field like face geometry along with quantum mechanism and handwritten Indian regional languages. To find out the points of face and calculate the distance as well as angles are used as secret message and authentication of a user. This generic method can increase the security level because it can work in various Indian regional languages and it have used a concept of Revised SSCE value and user's entered Passkey also. This can also prove the steganalysis attack. The results and analysis shows the best performance in this writings.

References

[1] F.A.P. Petitcolas, R.J Anderson, M.G. Kuhn: Information Hiding—A Survey, Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078, ISSN 0018-9219.

[2] R.J. Anderson., F.A.P Petitcolas. On the limits of steganography. IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection, 16:474–481, 1998.

[3] I. Banerjee, S. Bhattacharyya, G.Sanyal. "DWT Based Image Steganalysis". Journal on "World Academy of Science, Engineering and Technology (WASET), International Journal of Computer, Information, Systems and Control Engineering" published in International Science Index Vol: 8, No:8, 2014.

[4] Krista Bennett (2004). "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.

[5] I. Banerjee, S. Bhattacharyya, G. Sanyal, "An Approach of Quantum Steganography through Special SSCE Code", International Journal of Computer and Information Engineering (WASET), Vol:5, No:8, Year:2011.

[6] Jain.A.K, Hong.L, Pankanti.S: Biometric identification. Communications of the ACM 43 (2000) P. 91-98.

[7] A. K. Jain, A. Ross and S. Pankanti, Biometrics: A tool for information security, IEEE Transactions on Information Forensics and Security, vol.1, no.2, pp.125-143, 2006.

[8] K. A. Rhodes, Information Security: Challenges in Using Biometrics, United States General Accounting Office, 2003.

[9] A. K. Jain, A. Ross and S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol.14, no.1, pp.4-20, 2004.

[10] S. Prabhakar, S. Pankanti and A. K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security and Privacy, vol.1, no.2, pp.33-42, 2003.

[11] A. K. Jain and A. Kumar, Biometrics of next generation: An overview, The 2nd Generation Biometrics, 2010.

[12] J. Gea-Banacloche. Journal of Mathematical Physics, pp. 43, 4531, 2002.

[13] S. Natori. Quantum computation and information. Topics in Applied Physics (Springer, Berlin/Heidelberg), 102:235–240, 2006.

[14] K. Martin. Lecture Notes in Computer Science, pp. 4567, 32, 2008.

[15] M. Curty and D. J. Santos. 2nd Bielefeld Workshop on Quantum Information and Complexity, 2000.

[16] Nielsen, Michael A. & Chuang, Isaac L. (2000). Quantum Computation and Quantum Information. Cambridge University Press. ISBN 0-521-63235-8.

[17] Krista Bennett (2004). "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.

[18] J. Pedraza, M. A. Patricio, A. de Asís, and J. M. Molina, "Privacy and legal requirements for developing biometric identification software in context-based applications," International Journal of Bio-Science and Bio-Technology, vol. 2, no. 1, pp. 13–24, 2010.

[19] S. Mazumdar; V. Dhulipala. "Biometric Security Using Finger Print Recognition". University of California, San Diego. p. 3. Retrieved 30 August 2010.

[20] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.

[21] R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice, Wiley, ISBN 978-0-470-51706-2, 2009.

[22] M. Bača; P. Grd and T. Fotak (2012). "4: Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics". New Trends and Developments in Biometrics. InTech. Retrieved 1st December 2013.

[23] S. Song; K. Ohnuma; Z. Liu; L. Mei; A. Kawada; T. Monma "Novel biometrics based on nose pore recognition" 2009.

[24] S. Prakash, U. Jayaraman, P. Gupta, A Skin-Color and Template Based Technique for Automatic Ear Detection, Proceedings of 7th International Conference on Advances in Pattern Recognition (ICAPR 2009), pp. 213-216, Kolkata, India, February 2009.

[25] Yeung, D; H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G; "SVC2004: First international signature verification competition". Lecture Notes in Computer Science. LNCS-3072: 16–22. 2004.

[26] Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons." Proceedings of the IEEE, vol. 94 (11), 2006, pp. 1927-1935.

[27] H. Beigi, Speaker Recognition, Biometrics / Book 1, Jucheng Yang (ed.), Intech Open Access Publisher, 2011, pp. 3-28, ISBN 978-953-307-618-8.

[28] Wang, L.-Y., G. Leedham, and D. S.-Y. Cho, Infrared Imaging of Hand Vein Patterns for Biometric Purposes, The Institution of Engineering and Technology, Computer Vision, Vol. 1, pp. 113-122, 2007.

[29] Kumar, A., K. and K., V. Prathyusha, Personal authentication using hand vein triangulation, IEEE Trans. Image Process., Vol. 38, pp. 2127-2136, 2009.

[30] M. Shirali-Shahreza, "Text Steganography by Changing Words Spelling". 10th International Conference on Advanced Communication Technology, 2008. ICACT 2008. (Volume:3). pp. 1912 – 1913, ISSN : 1738-9445, Conference Location : Gangwon-Do, Date of Conference: 17-20 Feb. 2008, Publisher: IEEE.

[31] L.Y Por, K.O Chee, T.F Ang, D. Beh. "An enhanced embedding method using inter-sentence, inter-word, end-of-line and inter-paragraph spacing", International Journal of the Physical Sciences. Vol. 6(36), pp. 8130 - 8142, 30 December, 2011. ISSN 1992 - 1950 ©2011 Academic Journals.

[32] S. Khan, B. Abhijitha, R. Sankineni, B. Sunil. "Polish text steganography method using letter points and extension", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015. Date of Conference: 5-7 March 2015, pp. 1 – 5, Print ISBN: 978-1-4799-6084-2, Conference Location : Coimbatore, Publisher: IEEE.