iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5430

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

A Propose Model for Biometrics Authentication and Data Security

Radheshyam Gupta[1], Dr. Neelam Sahu[2]
[1, 2]*Information Technology, Dr. c.v. Raman University, Kota Bilaspur, India*

Abstract: ***We have difficult to remember long cryptographic keys for us and when we encrypt our data, cryptographic keys is provided by third party, so it can be shared to hacker. Therefore, for remove this problem, for a long time period, researchers have been discovers a new ways to use biometric features of the user which is memorable and totally independent from third party cryptographic keys provider. This effort to produce tough and unique cryptographic keys and to organize the key unpredictable to a hacker who is deficient of valued knowledge about the user's biometrics. In this paper, produce the powerful bio-crypt key based on fingerprint image processing algorithms. At first, fingerprint image converting into binary number format(zero(0) and one(1)). Then, converted binary number again converted into decimal number that used in cryptographic key.***

Keywords: Cryptography, Biometrics, Fingerprint, Encryption, Decryption key, Programming Language.

I. INTRODUCTION

Cryptography not only secure our data from theft or alteration, but it can also be used for user authentication. It is a technology key in electronic key systems. It is used to secure data secret, digitally sign documents, ingoing control, and so forth. Users therefore should not only know how its techniques work, but they must also be capable to estimate their efficiency and security. It is the technique for secretion data and information from unauthorized users. Cryptography can be separated into following three categories rest upon the types of key used: public key(asymmetric) cryptography, secret key (symmetric) cryptography and hash functions. The instantly continuous upgrowth in exchange of multimedia data over guarded and unguarded networks such as the worldwide accessible internet and local networks such as shared networks and local area networks etc has encouraged activities such as illegal usage, unauthorized access, disruption, stored data and alteration of transmitted. This widely spread use of digital media over the internet such as on cloud storage systems, on social media etc and over all other communication medium such as satellite communication systems have enhanced as applications and importance for systems to meet current and future circulation evolved over the years.

A. In Cryptography, there are some Important Terms with used in cryptography ,these are given below (figure 1)

1) Crypto Analyst: A person who is an expert in breaking and analyzing codes.

2) Plain Text: It is the original text which the user has to be encrypted with the help of key.

3) Cipher Text: It is secure encrypted text which obtained after encipher the data with the help of a key is known as cipher text.

4) Key: It is a word or variable value that is used to enciphering the plain text or decrypt the cipher text.

5) Encryption: The way of converting the plain text into coded form with the help of key is called encryption.

6) Decryption: The way of converting the encoded data to its original form or plain text with the help of decrypted key is called decryption.

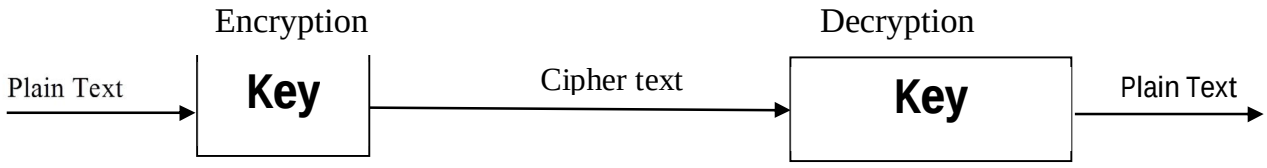


figure1: cryptographic

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. BIOMETRICS

A biometric system is identify as a measurable, unique, biological characteristic or trait for automatically verifying or recognizing the identity of a human being. Statistically analyzing these biological characteristics of human being has become known as the science of biometrics. These days, human characteristics are typically used to analyze for security purposes with the help of biometric technologies. Five human characteristics are the most common physical biometric patterns used for security purposes are the fingerprint, eye, hand, voice, and face given below (figure 2):

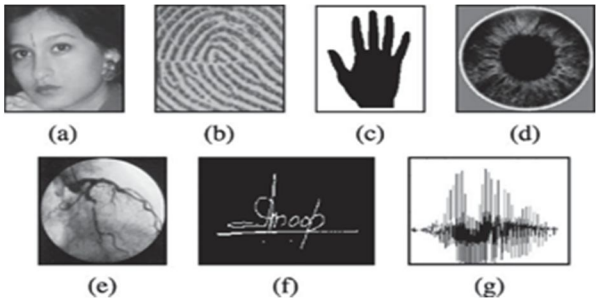


Figure 2: examples of the biometric characteristics. (a) fingerprint. (b) face.
(c) Handgeometry. (d) Iris. (e) Signature.(f) Retina. (g) Voice from d. maio, d. Maltoni, s. Prabhakar, a. k. jain , handbook of fingerprint recognition system

The use of biometric characteristics of human being as a means of identification is not a new concept in biometric system.Biometric system identification consists of two stages: first is enrollment the biometric characteristics and verification the biometric characteristics. During the first stage of enrollment , a sample of the designated biometric is acquired from human. Some unique biometric characteristics or features of this sample are then extracted to form a biometric template for purpose of subsequent comparison. At the time of verification stage, biometric updated sample is acquired. As in enrollment, extracted the features of this biometric sample . These biometric features are then compared with generated previously biometric template.

III. CRYPTO KEYS AND BIOMETRICS

Biometrics system offers a natural and reliable solution to certain aspects of authentication management by utilizing fully automated or semi-automated schemes to discriminate individuals based on their biological characteristics.

In traditional cryptography systems, user authentication is based on self generated secret keys, if the keys are not kept secret or forget then the method fails (i.e., shared with unauthorized users).

Further, keys can be lost, forgotten, or stolen and, thus, cannot provide non-reject. Now modern cryptography system based on physiological and behavioral characteristics of persons known as biometrics. Biometrics authentication systems such as fingerprints authentication systems, naturally provide solutions to many of these problems and may replace the traditional authentication component of traditional cryptosystems. Biometric cryptography systems are similar to password generation key based systems as they are used to more secure cryptographic key or to directly generate cryptographic key from human biometric features. Since the biometric measurements obtained during the time of enrollment and authentications both are different, these obtained biometric features cannot be directly used for the generation of cryptographic key. To facilitate generation of key helper data or secure sketch of the biometric features are stored during the time of enrollment. Therefore biometric cryptography technique are also known as helper data systems. The main reason to developed biometric cryptography systems for the purpose of either securing a cryptographic key for encryption and decryption using biometric features or directly generating a cryptographic key with the help of biometric features.

Note that Biometric Encryption technique refers to a process of secure key management which are not required to store in database. Biometric Encryption mechanism does not provide encryption/decryption of data directly, but rather provides a replacement protocols to typical pass-code key-protection protocols. Specifically, With the help of Biometric Encryption, it provides a secure method for key management in cryptography system to complement existing cipher systems.

Although the process of Biometric Encryption technique can be applied to any human biometric image, using fingerprint images the initial implementation was achieved. The application of the Biometric Encryption algorithm to other biometrics feature such as eye,

hand, voice, and face. Biometric Encryption using other biometric feature templates show overall mechanism show in (figure 3) for biometric cryptography.

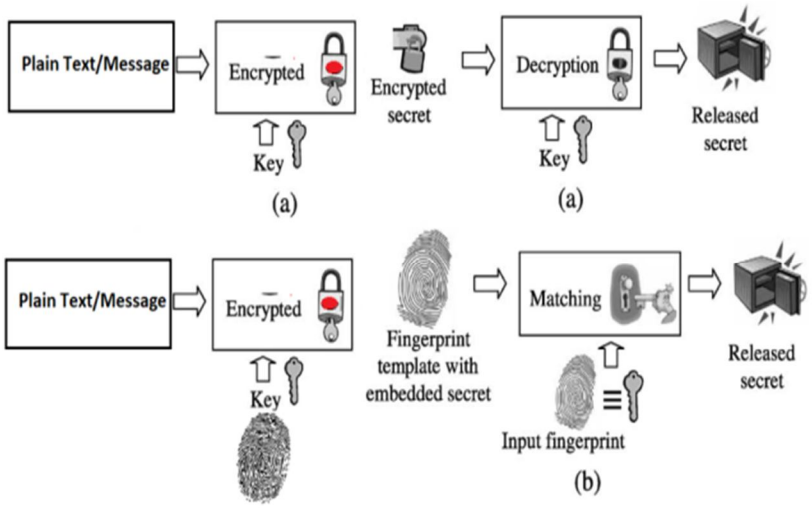


Figure 3: Overall mechanism for biometric cryptography.

IV. REVIEW OF LITERATURE

Till now there are huge amount of work done by the various researchers in the field of bio-cryptographic algorithm for data security. Some of these work which done by the researchers are explain below:

Sarita K (2017) have described Cryptography protects users by providing functionality for the encryption of data and authentication of other unauthorized users. Cipher is the algorithm for encryption that is used to convert plaintext to cipher text which is not understandable by unauthorized user, This method is called encryption phase of cryptography, in another words, it's a mechanism of transform readable and understandable data into "meaningless" data which is not understandable by unauthorized user.

Neha S *et al*. (2017) have described cryptography algorithms like symmetric key algorithm like DES, AES, blowfish and algorithm for Asymmetric key like Diffie–Hellman key exchange algorithm, RSA. Use encryption and decryption in any type of public application for exchanging confidential data in worldwide network.

Kumar K. *et al*. (2017) have described Image and Text encryption decryption using advanced Encryption Standard technique". In this paper they described that the size of images data have large data size and also has real time restrict problem hence the similar technique cannot be used to preserve images as well as text from unauthorized person access. However with few variations in technique AES can be used to preserve image as well as text unauthorized person access. Using AES methods, they had implemented encryption and decryption on text and image.

B.J.Jisha Nair.(2015)have described by using biometrics data it is possible to establish an identity based on user who you are, rather than by what you possess for identity , such as an identity card, or what you remember for authentication, such as a password key. In some bio-applications, biometrics may be used like supplement identity cards and passwords key thereby imparting an additional level of security for identity. Biometrics system offers a natural and reliable solution to certain aspects of identity management system by utilizing fully automated or semi-automated mechanism to recognize by their individuals based biological characteristics .Secure sketch is public data about biometric characteristics stored in databases during [process of enrollment time. Biometric cryptography systems are categorized as key release, key binding and key generation systems depending on how the secure sketch is obtained for biometric device.

Durairajan M.S.*et al*. (2014) have described the finger print value of the sender and receiver are converted to like decimal value. The finger print decimal value of sender and receiver obtained from the biometric authentication capture device which is used decimal value as the private key. In biometric this method is used for exchanging secret crypto key between two user and ensures that both authentication and non-repudiation. Here, used encryption scheme based on Diffie-Hellman, instead of exchanging secret key, finger print of person data is stored in database, at the time of authentication it is only retrieved, and no one can show as a sender, because of his unique finger print identity value. This works submit the cryptanalysts under the pressure. The use of this novel biometric algorithm in biometric signature creation reform the electronic banking security, Use biometric technique the public

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

and private keys are created without storing in database and exchanging any private information anywhere over the worldwide network.

V. RESEARCH METHODOLOGY

The bio-crypto study is an attempt to explore Biometric cryptography and its level of encryption and decryption. It results in the encryption and decryption of the biometric images data and its defacement and histogram equalization of cryptography.
The study consisted of one variants biometric images thumb . biometric images was collected from different biometric images sample of 24 samples of distinct pixel size and image size.
In this cryptographic, i not use any cryptographic algorithm For encryption & decryption. Data/information can be encoded utilizing "Biometric data" technology in cryptography. For encryption & decryption, i use "finger Print" in place of keys. In experimental work, here the total technique is discussed in some individual steps, at first at receiver's side and then at sender's side.
In this proposal, I use biometric data in the place of "Key". this proposal, I remove third party involvement for Key.
First capture fingerprint image from biometric device and convert finger print image value in Binary number (show below in figure 4) , after getting binary number then again convert this value in decimal number .

Figure 4:convert fingerprint image data into binary number

VI. EXPERIMENTAL WORK

In this cryptographic, i not use any cryptographic algorithm For encryption & decryption. Data/information can be encoded utilizing "Biometric" technology .For encryption & decryption, i use "finger Print" in place of keys. Below, here the total technique is discussed in some individual steps, at first at receiver's side and then at sender's side.

A. Steps At Receiver's Side

At receiver's end, generate his finger print image with the help of biometric device and send this finger print image to sender.

B. Steps At Sender's Side

Indexing the document letter in Tabular Form
Suppose my .txt file name is 'crypt.txt', who have following word are available
"What is Document? Do You Know.##**"** **.**
First, we have to count the total number of letter including space present in out .txt document and count total number of unique letter in .txt document.
Second, we have to create one dimensional array (A[count value of total latter]) for getting the place value of latter. Show (figure 5)
Third, we have to create two dimensional array (B[unique letter value][2]) for getting highest count value of similar latter. Show (figure 6)
Third, we have to search the highest value from Array B.
Fourth, we have to create two dimensional array (C[unique letter value][2+ highest value of number which we get from first array]) for storing the document's letter in tabular form.
Show (figure 7) the **place value** of each **Similar Letters** and Show (figure 8) the Indexing document text in **tabular** form.

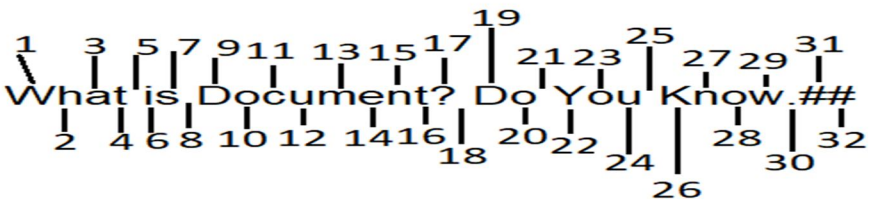


Figure 5: place value of letters

W	1
h	1
a	1
t	2
	5
i	1
s	1
D	2
o	4
c	1
u	2
m	1
e	1
n	2
?	1
Y	1
k	1
w	1
.	1
#	2

Figure 6: Getting Highest Count Value Of Similar Latter

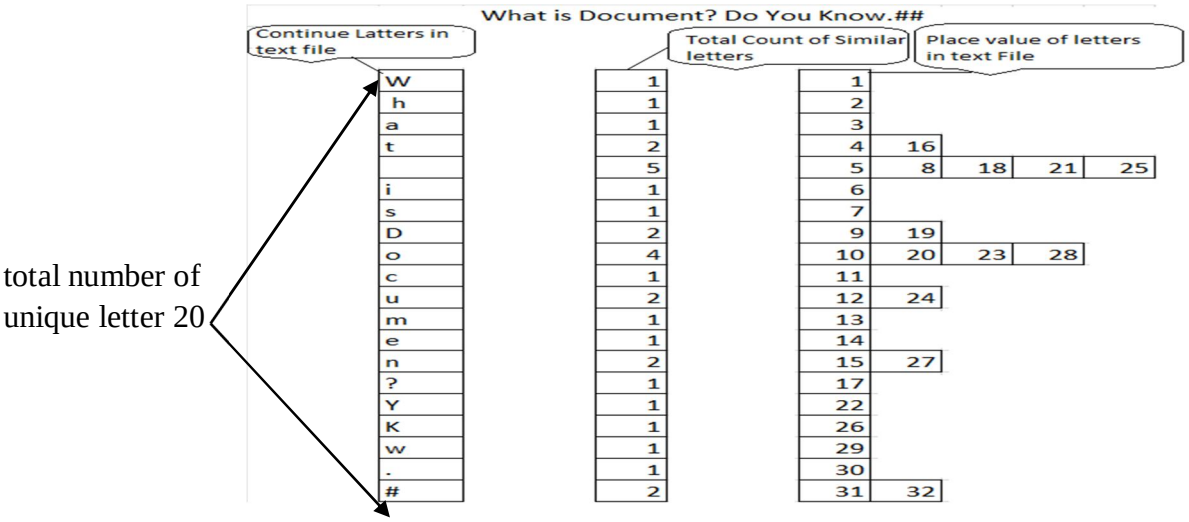


Figure 7:indexing document plain text in tabular form.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Overall mechanism show below in (figure 8) which used in figure 5, figure 6 and figure 7 Array C[unique letter value][2+ highest value of number which we get from first array] C[20][7]

W	1	1				
h	1	2				
a	1	3				
t	2	4	16			
	5	5	8	18	21	25
i	1	6				
s	1	7				
D	2	9	19			
o	4	10	20	23	28	
c	1	11				
u	2	12	24			
m	1	13				
e	1	14				
n	2	15	27			
?	1	17				
Y	1	22				
k	1	26				
w	1	29				
.	1	30				
#	2	31	32			

Figure 8: Plain text in array.

1) *Fingerprint Image Data:* We need to collect the sender & receiver fingerprint data image from finger print Scanner devices. After capturing the fingerprint image data, we have to convert the fingerprint image data into Binary number format .After converting in binary number format, again we have to convert binary number format into Decimal number format.Basic mechanism are given below (figure 9).

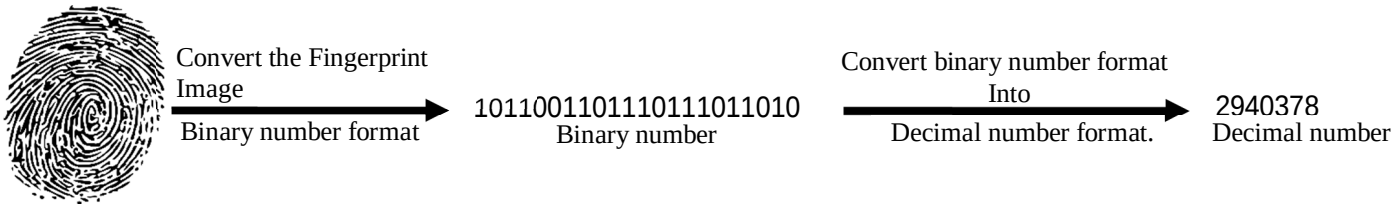


Figure 9:convert fingerprint image data into binary and binary to decimal.

2) *1'st phase Encryption Process:* After completion of above Process, now we have to start the process of encryption process.
We use mathematical multiplication operation for encryption. Below (figure 10).
I use Decimal value as a "Key" for Encryption.
I multiply decimal value (decimal value getting after converting sender & receiver fingerprint image data).
I multiply sender fingerprint image decimal value from total count index table value and receiver fingerprint image decimal value from place value of index table.

Suppose i getting decimal value of sender fingerprint image 2 and 3 decimal value from receiver.
Basic mechanism are given below (figure 10).

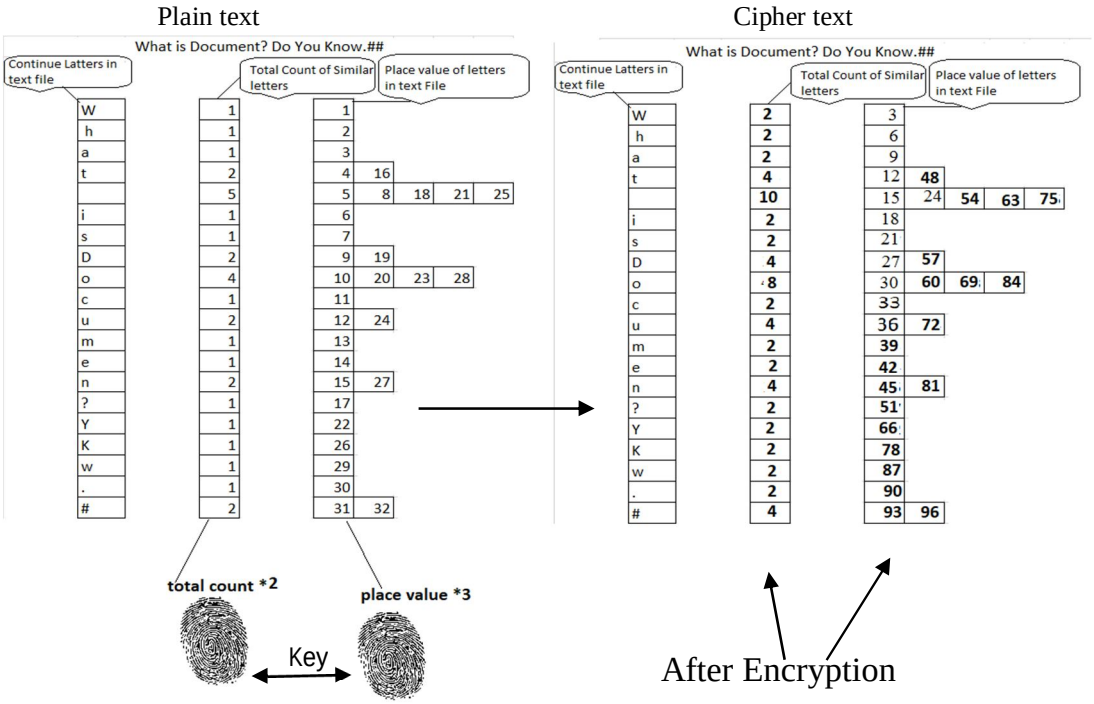


Figure 10:encryption process

After finish the encryption process, again we have to find big count value from total count of similar latter column.
Getting big count value, we create two dimensional array.
Array D[unique letter value][2+ highest count value]
D[20][12]
And put the value like below in (figure 11) in newly created array.

W	2	3									
h	2	6									
a	2	9									
T	4	12	48								
	10	15	24	54	63	75					
I	2	18									
S	2	21									
D	4	27	57								
o	8	30	60	69	84						
c	2	33									
u	4	36	72								
m	2	39									
e	2	42									
n	4	45	81								
?	2	51									
Y	2	66									
k	2	78									
w	2	87									

.	2	60									
#	4	93	96								

Figure 11: cipher text in array

3) *2'nd phase Algorithms for Encryption Process:* After complete` the above process, we have need to fill all the blank cell of array.

a) Start from cell index 3

b) Check index 3 is Null, if not Null ,then jump in next index of array, If index 3 is Null, Put 1 value in index 3 And check index 3 value is equal/not to index 2 value till form last index value of array. If match, increase the value with one(1++) and again check from index 2 from till last index value of array. If not match or equal the value of index 3 from any index value then jump next index(3+1).

c) Now again repeat the step a and b, till the we not get a single index is empty in array. After finish the above process, we get fully finish Cipher text in array ,show in (figure 12)

W	2	3	1	2	4	5	7	8	10	11	13
h	2	6	14	16	17	19	20	22	23	25	26
a	2	9	28	29	31	32	34	35	37	38	40
T	4	12	48	41	43	44	46	47	39	50	52
	10	15	24	54	63	75	53	55	56	58	59
I	2	18	61	62	64	65	67	68	70	71	73
S	2	21	74	76	77	79	80	82	83	85	86
D	4	27	57	88	89	90	91	92	94	95	97
o	8	30	60	69	84	98	99	100	101	102	103
c	2	33	104	105	106	107	108	109	110	111	112
u	4	36	72	113	114	115	116	117	118	119	120
m	2	39	121	122	123	124	125	126	127	128	129
e	2	42	130	131	132	133	134	135	136	137	138
n	4	45	81	139	140	141	142	143	144	145	146
?	2	51	147	148	149	150	151	152	153	154	155
Y	2	66	156	157	158	159	160	161	162	163	164
k	2	78	165	166	167	168	169	170	171	172	173
w	2	87	174	175	176	177	178	179	180	181	182
.	2	60	183	184	185	186	187	188	189	190	191
#	4	93	96	192	193	194	195	196	197	198	199

Figure 12: cipher text in array

After complete this above process, export this array in excel format and send this excel file and sender fingerprint to receiver.

C. Steps At Receiver's Side

1) *1'st Phase Decryption process:* Export excel file in array show in (figure 13)

W	2	3	1	2	4	5	7	8	10	11	13
h	2	6	14	16	17	19	20	22	23	25	26
a	2	9	28	29	31	32	34	35	37	38	40
T	4	12	48	41	43	44	46	47	39	50	52
	10	15	24	54	63	75	53	55	56	58	59
I	2	18	61	62	64	65	67	68	70	71	73
S	2	21	74	76	77	79	80	82	83	85	86
D	4	27	57	88	89	90	91	92	94	95	97
o	8	30	60	69	84	98	99	100	101	102	103
c	2	33	104	105	106	107	108	109	110	111	112
u	4	36	72	113	114	115	116	117	118	119	120
m	2	39	121	122	123	124	125	126	127	128	129
e	2	42	130	131	132	133	134	135	136	137	138
n	4	45	81	139	140	141	142	143	144	145	146
?	2	51	147	148	149	150	151	152	153	154	155
Y	2	66	156	157	158	159	160	161	162	163	164
k	2	78	165	166	167	168	169	170	171	172	173

w	2	87	174	175	176	177	178	179	180	181	182
.	2	60	183	184	185	186	187	188	189	190	191
#	4	93	96	192	193	194	195	196	197	198	199

Figure 13: cipher text in array

2) 2'st phase Decryption process

a) Get index 1 value form array (in this array we get 2 from starting position) Keep the value for index 1+index 1 value and remove remaining element form next index.

b) Repeat step 'a' till end of row .After finish the above process, we get fully finish Cipher text in array ,show in (figure 14)

W	2	3									
h	2	6									
a	2	9									
T	4	12	48								
	10	15	24	54	63	75					
I	2	18									
S	2	21									
D	4	27	57								
o	8	30	60	69	84						
c	2	33									
u	4	36	72								
m	2	39									
e	2	42									
n	4	45	81								
?	2	51									
Y	2	66									
k	2	78									
w	2	87									
.	2	60									
#	4	93	96								

Figure 14: cipher text in array

3) 3'st phase Decryption Process: Divide the sender fingerprint decimal value(2) from Column 2 and remaining columns divided form receiver fingerprint decimal value(3) .

Basic mechanism are given below (figure 15 and 16).

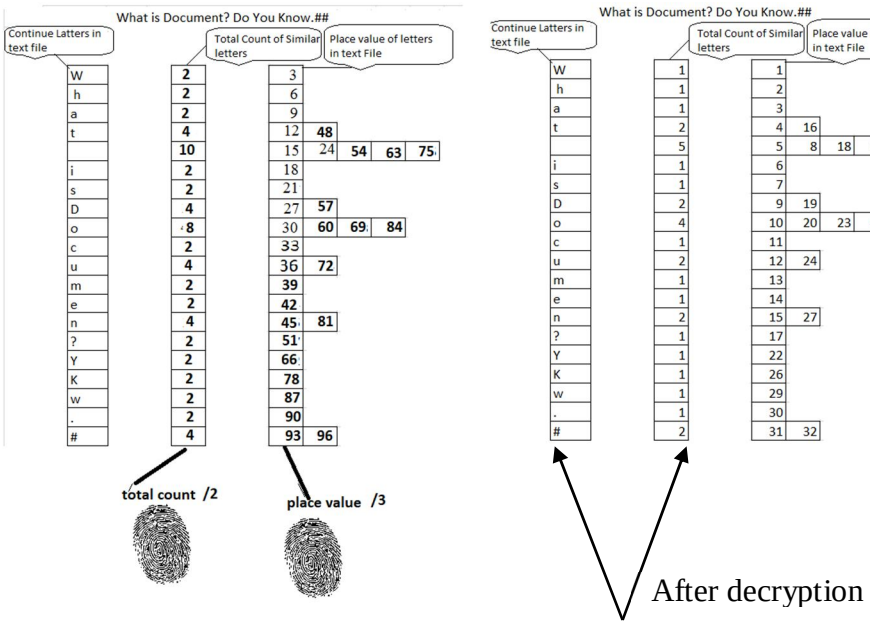


Figure 15: Decryption process

W	1	1				
h	1	2				
a	1	3				
t	2	4	16			
	5	5	8	18	21	25
i	1	6				
s	1	7				
D	2	9	19			
o	4	10	20	23	28	
c	1	11				
u	2	12	24			
m	1	13				
e	1	14				
n	2	15	27			
?	1	17				
Y	1	22				
k	1	26				
w	1	29				
.	1	30				
#	2	31	32			

Figure 16: decryption process

After complete this above process, export this array in text format like this show below in (figure 17).

VII. CONCLUSION AND FUTURE WORK

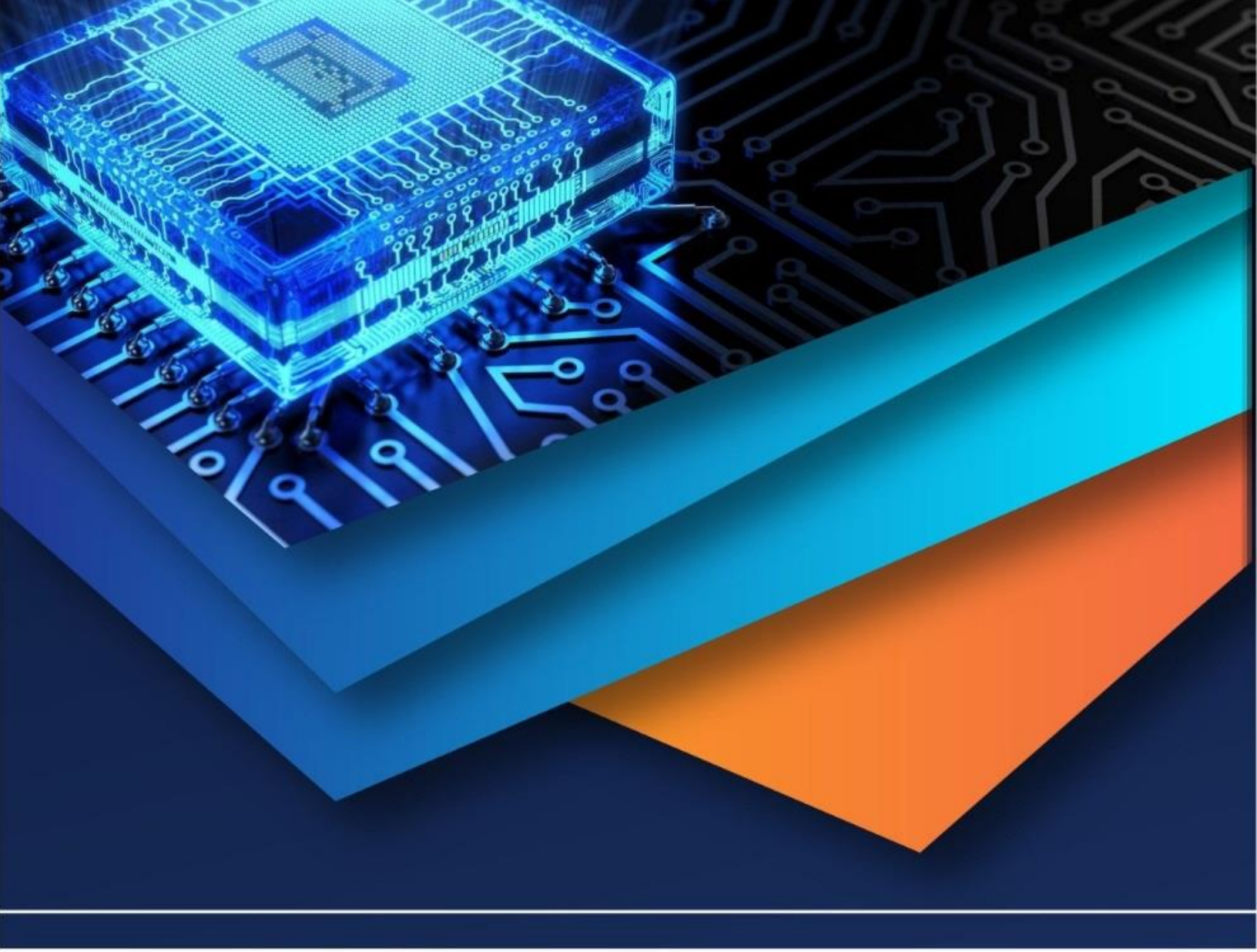
In this Experiment, a new technique is developed with the help of human biometric fingerprint data. The objective of this study is to develop a system to sure data from unauthorized user with the help of fingerprint data. With the help of fingerprint data we create encryption and decryption key for protect our private data from unauthorized user. When we use the fingerprint data as a key, key not required to store in database and not required to remember it and it also independent from third party key provider. All human being biometric data are different from each other, so that the biometric key is unique and not a single chance to match with another user.

Use this technique we get totally different from traditional cryptography system. The following conclusion we get form this research these are given below.

1) Remove third party involvement in the process of encryption & decryption for "Key".
2) User depend on self for encryption & decryption key, for this, nobody can understand the transferred received message except the one who has authorized and the decipher key and only authorized receiver has decipher key.
3) Biometrics data is unique data, if we use Biometrics data as a key for encryption & decryption, no one can access/ understand our transferred data .
4) Provide very high level security for data authentication . So our data will secure and save from unauthorized user.

REFERENCES

[1] Sarita K (2017), A research Paper on Cryptography Encryption and Compression Techniques, International Journal Of Engineering And Computer Science, 6(4), 20915-20919, ISSN:2319-7242
[2] Neha S, Prabhjot(2017), A Review of Information Security using Cryptography Technique,International Journal of Advanced Research in Computer Science,8(4),323-326,ISSN:0967-5697.
[3] Kumar K.(2017) , A Review Paper on Cryptography for Data Security,International Journal for Research in Applied Science & Engineering Technology (IJRASET) ,5(5),250-255,ISSN: 2321-9653
[4] B.J. Jisha Nair.(2015),A Review on Biometric Cryptosystems,International Journal of Latest Trends in Engineering and Technology,6(1),46-53,ISSN: 2278-621X.
[5] Durairajan M.S., Dr.R. Saravanan(2014),Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism,International Journal of ChemTech Research CODEN,6(9),4359-4365, ISSN : 0974-4290.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY