TITLE:

Image Encryption Based on Algebraic S-box and Galios Field

Team:

ABDUL MOHSIN SIDDIQI (14BCS0036)

ZAKI MUSTAFA FAROOQUI (14BCS0050)

MOHD. ZAIYAN ALAM (14BCS0041)

ABSTRACT

In this research project, we are going to work on an effective image encryption algorithm using S-Box and Galois field. Broadly speaking, our work will comprise of three major tasks to be performed, which are discussed below:

- IMAGE ENCRYPTION

  The very first step involved is the generation of an efficient and fast S-BOX which can efficiently encrypt an image. S-BOX generation involved choosing optimal initial condition and generator function to get an efficient S-BOX. The image to be encrypted is first converted into bits encoding and then these encoded bits are used to generate the corresponding S-Box.

- ALGORITHM PERFORMANCE ANALYSIS

  After successfully generating our S-box, we then apply our own S-box based Image Encryption Algorithm in order to efficiently and successfully perform encryption. Next, we perform analysis on performance and statistics on our algorithm through a set of parameters such as entropy, homogeneity, contrast, energy etc, and later correlate the results so obtained. Additionally, we will also perform differential analysis in order to show high sensitivity to single-bit change in the plain images.

- ATTACK ON EXISITING ALGORITHM

  Our Final major step would be to analyze the algorithm devised in Shabieh Farwa's paper work and point out noticeable flaws. We will perform security analysis on the existing algorithm and show that it isn't highly secured and also vulnerable making it insecure for communication. Further, we will prove it by demonstration through simulation techniques and associated significant references.

INTRODUCTION

In this research project, we are going to work on few pre-existing fields and algebraic structure which are as explained below:

GALIOS FIELD

- Let F be a set of objects on which two operations + and . are defined,
- F-{0} forms a commutative group under .
- The multiplicative identity element is labeled '1'. 3.
- The operation + and . distributes: a . (b+c)=(a .b)+(a .c)
- A field with finite number of elements is called a finite field, also called Galois Field, denoted by GF(p). p can be a prime number or power of prime.

Examples of Galios(Finite) Fields

- Finite field GF(2) consists of elements 0 and 1 '+' XOR operation additive identity: 0 '.' AND operation; multiplicative identity:
- Finite field GF(7) consists of elements 0,1, …6 '+' mod 7 integer addition additive identity: 0 '.' mod 7 integer multiplication multiplicative identity:

S-BOX

- S-BOX stands for substitution box (S-box) which is an algebraic structure represented by an 8x8 vectorial Boolean matrix.
- Substitution box (S-box) is a standout in symmetric key cryptography and is a widely used mechanism in any substitution-permutation network as a source to produce nonlinearity ,
- Many algorithms have been presented for the construction of safer and more reliable S-boxes. In addition, applications of S-boxes in digital image encryption, steganography and watermarking have become quite popular and influential in recent years. Zhang et al. studied the S-box-only.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

ALGORITHM/TECHNIQUES USED

Improvisation on Shabieh Farwa work of "A Novel Image Encryption Based on Algebraic S-box and Arnold Transform":

- **Step 1**: Improvement(1) on S-box Generation:

-Apply some algorithm Group strategy (power of generator g; right now we are taking g's power = 8)
-Use this strategy to generate our S-box where the power of g can be randomly generated within the range [0,255] using Chaos based Algorithm (because of its most dominating feature of sensitivity towards the initial conditions)
-Record the local best S-box value in each iteration and compare each of the local best with the global best S-box.
-Search the global best for large number of iterations (and hence, generation of S-box)

- **Step 2**: Improvement(2) on Image Encryption:

-Apply the proposed Image Encryption Procedure based on S-box for improved S-Box based encryption.
-Perform Performance and Statistical analysis (for visualization of results, using histograms) by taking into account the following Parameters:

- Entropy
- Non-Linearity
- Contrast
- Homogeneity (using Gray level co-occurrence matrix (GLCM))
- Energy, etc.

-Perform Correlation analysis on different sets of plain and encrypted images.
-Perform Differential Analysis using following measures:

- NPCR
- UACI

-Lastly, perform the Computational cost comparision (Time Analysis)

- **Step 3**: Cryptanalysis

-Involves Security Analysis on the existing work of Sabeih Farwa's Encryption Algorithm and report certain vulnerabilities and flaws in order to show that it is insecure for communication.
-Comparative Analysis of our own algorithm to that of the existing one and determine efficiency of each method.
-Employment of Simulation techniques in order to prove our basis and providing associated references.

PROGRAMMING ENVIRONMENT AND TOOLS USED

1. Python IDE/ Matlab(Octave) (For Procedure Implementation)
2. Jupyter Notebook
3. Matplotlib (For Statistical Analysis and Visualization)

REFERENCES

1. Shabieh Farwa . Nazeer Muhammad . Tariq Shah . Sohail Ahmad (July 2017)
"A Novel Image Encryption Based on Algebraic S-box and Arnold Transform",
Published at 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany

- LINKS
http://faculty.washington.edu/manisoma/ee540/EE540finite.pdf
http://crypto.stackexchange.com/questions/2700/galois-fields-in-cryptography
https://en.wikipedia.org/wiki/Finite_field_arithmetic
http://www.samiam.org/rijndael.html
http://web.eecs.utk.edu/~plank/plank/papers/CS-07-593/
https://www.doc.ic.ac.uk/~mrh/330tutor/ch04s02.html
https://www.doc.ic.ac.uk/~mrh/330tutor/