INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

सत्यमेव जयते
GOVERNMENT OF INDIA

Controller General of Patents,Designs and Trademarks
Department of Industrial Policy and Promotion
Ministry of Commerce and Industry

Application Details

APPLICATION NUMBER	202041002481
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	20/01/2020
APPLICANT NAME	1 . Dr. Babu Rao Markapudi 2 . Dr. Kavitha Chaduvula 3 . Dr. Chaduvula. Rathna Jyothi 4 . Yadlapalli Kasiviswanadham 5 . Melam Naga Raju
TITLE OF INVENTION	COMPUTER IMPLEMENTED METHOD FOR ENHANCED SECURITY OF COLOR IMAGE USING ASYMMETRIC RSA ALGORITHM
FIELD OF INVENTION	COMMUNICATION
E-MAIL (As Per Record)	baburaompd@gmail.com
ADDITIONAL-EMAIL (As Per Record)	baburaompd@gmail.com
E-MAIL (UPDATED Online)	
PRIORITY DATE	NA
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	31/01/2020

Application Status

APPLICATION STATUS	**Application Published**

View Documents

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 05//2020	शुक्रवार	दिनांक: 31/01/2020
ISSUE NO. 05/2020	FRIDAY	DATE: 31/01/2020

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :20/01/2020

(21) Application No.202041002481 A
(43) Publication Date : 31/01/2020

(54) Title of the invention : COMPUTER IMPLEMENTED METHOD FOR ENHANCED SECURITY OF COLOR IMAGE USING ASYMMETRIC RSA ALGORITHM

(51) International classification :H04L0029060000,H04L0009300000,H04L0009080000,G06F0021600000,A61B0006020000
(31) Priority Document No :NA
(32) Priority Date :NA
(33) Name of priority country :NA
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Dr. Babu Rao Markapudi
Address of Applicant :Professor,Department of Computer Science and Engineering, Gudlavalleru Engineering College, Gudlavalleru-521356, Krishna district, Andhra Pradesh, India Andhra Pradesh India
2)Dr. Kavitha Chaduvula
3)Dr. Chaduvula. Rathna Jyothi
4)Yadlapalli Kasiviswanadham
5)Melam Naga Raju
(72)**Name of Inventor :**
1)Dr. Babu Rao Markapudi
2)Dr. Kavitha Chaduvula
3)Dr. Chaduvula. Rathna Jyothi
4)Yadlapalli Kasiviswanadham
5)Melam Naga Raju

(57) Abstract :
The present invention is related to computer implemented method for enhanced security of color image using asymmetric RSA algorithm. The objective of present invention is to solve the anomalies presented in the prior art techniques related to security of color image using asymmetric RSA algorithm. It is disclosed in the disclosure that image files are encrypted and decrypted using RSA algorithm to improve the security before transferring/ receiving them in/from the communication channel. An image file is selected to perform encryption and decryption using key generation technique to transfer the data from one destination to another. This approach provides high security and it will be suitable for secured transmission of images over the networks or Internet.

No. of Pages : 21 No. of Claims : 4

FORM 2

THE PATENTS ACT, 1970

(39 of 1970)&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See section 10, rule 13)

1. TITLE OF THE INVENTION:

COMPUTER IMPLEMENTED METHOD FOR ENHANCED SECURITY OF COLOR IMAGE USING ASYMMETRIC RSA ALGORITHM

2. APPLICANTS

Sr.No.	Name	Nationality	Address
1	Dr. Babu Rao Markapudi	India	Professor,Department of Computer Science and Engineering, Gudlavalleru Engineering College, Gudlavalleru-521356, Krishna district, Andhra Pradesh, India
2	Dr. Kavitha Chaduvula	India	Professor, Department of IT, Gudlavalleru Engineering College, Gudlavalleru-521356, Krishna district, Andhra Pradesh, India
3	Dr. Chaduvula. Rathna Jyothi	India	Associate Professor, Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Enginnering, L.B.Reddy Nagar, Mylavaram-521230, Krishna district, Andhra Pradesh, India
4	Yadlapalli Kasiviswanadham	India	Associate Professor, Department of IT, Gudlavalleru Engineering College, Gudlavalleru-521356, Krishna district, Andhra Pradesh, India
5	Melam Naga Raju	India	Assistant Professor, Department of IT, Gudlavalleru Engineering College, Gudlavalleru-521356, Krishna district, Andhra Pradesh, India

3. PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION

The following specification particularly describes the invention and the manner in which it is to be performed.

COMPUTER IMPLEMENTED METHOD FOR ENHANCED SECURITY OF COLOR IMAGE USING ASYMMETRIC RSA ALGORITHM

FIELD OF INVENTION

The present invention is related to field of security of image transmission.

Particularly, the present invention relates to color image encryption system and method for images privacy authentication.

More particularly, the present invention is related to a computer implemented method for enhanced security of color image using asymmetric RSA algorithm

BACKGROUND & PRIOR ART

The subject matter discussed in the background section should not be assumed to be prior art merely as a result of its mention in the background section. Similarly, a problem mentioned in the background section or associated with the subject matter of the background section should not be assumed to have been previously recognized in the prior art.

The subject matter in the background section merely represents different approaches, which in-and-of-themselves may also be inventions.

The vital transfer of pictures can crop up in an unsecured web network. Therefore, there's a necessity for acceptable security in order that the image prevents access by the unauthorized person to special data.

Cryptography may be a kind of image security technique; it offers the secure method of transmittal and storing the image on the net. Security is the main concern of any system to maintain the integrity, confidentiality and authenticity of the image.

Some of the prior work is listed herewith:

IN3763CHE2015A - *video mosaic image creation for secure secret image transmission* presents transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly lossless from the mosaic image. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

IN201741041153A - *spherical image encryption (spie) for secured image storage* presents system, method for Spherical Image Encryption (SPIE) for Secured Image Storage. The proposed algorithm is able to encrypt JPG images and other non gif images. If a text document with text of small size is saved in image format and encrypted with proposed SPIE algorithm then it will take thousands of years to predict the content of the image. The security of image depends upon the secrecy of the encryption string; as if the consecutive values do not have large difference then the prediction will be easy by examining encrypted image. If we choose 1 thousand prime numbers for generation of encryption string (s) then the possible number of combinations will be 1 million (1000 1000). On an average it takes 3 minutes to encrypt or decrypt the image on a personal computer with normal configurations. To apply all possible combinations of encryption string (s), it will take 5.7870 years for generation of all possible combination of image. The time complexity of the algorithm run will depend on the value of V (not on its length) and the height of the image.

AU2018102042A4 - *A color image encryption based on optical chaos and secure sharing in cloud* presents convenient services to sharing and usage of images resource, but brings a threat to images security and privacy authentication. In this patent, we propose a color image encryption system based on two mutually coupled semiconductors lasers (MC-SL1 and MC-SL2) for secure resource sharing, and introduce a watermarking method for images privacy authentication in cloud. Two MC SLs are used to

transmit encryption/decryption key space generated by chaotic signal of MC-SL1 and user's key after achieving chaos synchronization under proper parameters. Before secure resource sharing in cloud, we carry out digital watermarking and encryption of a color image. On the other side of cloud, some tests are made for decryption of color image by received key space and watermark extraction.

CN100392675C - Method for hiding and excavating bottom image and device thereby presents method, which is characterized by comprising the following steps: step 1, Image hiding technique, the hidden original Image; step 2, a hidden Image hidden gray scale/color spectrum, excavation hidden Image gradation/chrominance information; step 3, the excavation hidden Image. One kind is used for the bottom layer of the device Image hiding and excavating, characterized in that wherein the central processing mechanism is connected with the Image information detection mechanism, Image information excavating and hidden mechanism is connected and a man-machine dialogue mechanism, the central processing mechanism also with the outside is connected with the Image identification mechanism. The invention has the remarkable effect is: can realize the safe and reliable text, Image encryption, secure transmission and decryption means.

TWI452890B - *chaotic image encryption method for cloud album* presents a chaotic image encryption method for a cloud album. Primarily, it comprises the following steps: taking at least one value of a multi-primary

color element of each pixel of an image when a user logins into a server end of the cloud album and sends the image to the cloud album; generating a chaotic sequence of the value of the multi-primary color element corresponding to the image pixel by means of a nonlinear differential equation module; proceeding with rank replacement with the chaotic sequence for each pixel of the image; proceeding with mod operation for each pixel completed with the rank replacement and the chaotic sequence to obtain each encrypted pixel; converting each encrypted pixel into an encrypted image.

CN107734208A - *Color image encryption and decryption method based on HSV space* presents a color image encryption and decryption method based on an HSV space. The method has a very good encryption effect on color images, and can resist against brute attacks and differential attacks, and more prominently, the encryption and decryption speed is much higher than those of an RGB space and an L * a * b * space. The conversion speeds of the RGB with the HSV and the L* a * b * color space are compared for the first time, and the high color image encryption and decryption speed based on the HSV space is verified. According to the color image encryption and decryption method, the different information amounts contained in three channels of HSV are considered, encryption methods with different complexity are adopted separately, thereby not only ensuring the security, but also improving the encryption and decryption speed.,

CN108898539A - *Color image encryption method compatible with JPEG compression standard* presents a color image encryption method that facilitates JPEG compression. The color image encryption method comprises the following steps: dividing an image to be encrypted I0 into n sub-blocks that do not overlap each other, and taking the first pixel of each sub-block to form an image I0'; using the SHA3-256 algorithm to calculate a hash value of the I0' and converting the hash value into a key in bits; using the Logistic map iteration to generate chaotic sequences and converting the chaotic sequences into pseudo-random sequences SK1, SK2, SK3, SK4, SK5; and using these sequences to perform the following operations on each plaintext image block in order: using the SK1 to control and scramble the relative position between sub-blocks; using SK2 to transpose and invert three color component matrices; using the SK3 to scramble the relative position between the three color component matrices of each sub-block; using theSK4 to perform vertical or horizontal cyclic shifting on each color component matrix of each sub-block.

CN110086953A - *Color image encryption method based on QR decomposition and Gyrator transformation* presents digital image processing and optical encryption, and provides a novel color image encryption method which has a large secret key space and high security. The color image encryption method based on QR decomposition and Gyrator transformation comprises the following steps: an image encryption part: encoding R and G color channels into a complex matrix, and decomposing

the obtained complex matrix into a normal orthogonal matrix Q and an upper triangular matrix R through QR; respectively carrying out GT (Gyrator) transformation on the Q part and the R part and then multiplying the Q part and the R part; performing phase truncation on an obtained result, encoding the result and the channel B into a complex matrix, and decomposing the complex matrix into Q and R parts through QR; respectively carrying out GT transformation on the Q part and the R part, and performing multiplying to obtain a final encrypted images.

CN109951278A - *Asymmetric digital image encryption method based on generalized chaotic synchronization system* presents an asymmetric digital image encryption method based on a generalized chaotic synchronization system, which comprises the following steps: firstly, constructing a four-dimensional chaotic system as a driving system, and designing a four-dimensional homoembryonic transfer function to generate a corresponding GCS response system; analyzing nonlinear dynamic characteristics ofthe GSC system; an asymmetric digital image secure communication scheme is provided. Carrying out GCS sequence full confusion scrambling on the 24-bit true color image; an original image is expanded to 48 bits, safety analysis is carried out through a key space.

Groupings of alternative elements or embodiments of the invention disclosed herein are not to be construed as limitations. Each group member can be referred to and claimed individually or in any combination with other

members of the group or other elements found herein. One or more members of a group can be included in, or deleted from, a group for reasons of convenience and/or patentability. When any such inclusion or deletion occurs, the specification is herein deemed to contain the group as modified thus fulfilling the written description of all Markush groups used in the appended claims.

As used in the description herein and throughout the claims that follow, the meaning of “a,” “an,” and “the” includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein, the meaning of “in” includes “in” and “on” unless the context clearly dictates otherwise.

The recitation of ranges of values herein is merely intended to serve as a shorthand method of referring individually to each separate value falling within the range. Unless otherwise indicated herein, each individual value is incorporated into the specification as if it were individually recited herein. All methods described herein can be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context.

The use of any and all examples, or exemplary language (e.g. “such as”) provided with respect to certain embodiments herein is intended merely to better illuminate the invention and does not pose a limitation on the scope of the invention otherwise claimed. No language in the specification should

be construed as indicating any non-claimed element essential to the practice of the invention.

The above information disclosed in this Background section is only for enhancement of understanding of the background of the invention and therefore it may contain information that does not form the prior art that is already known in this country to a person of ordinary skill in the art.

SUMMARY

The present invention mainly cures and solves the technical problems existing in the prior art. In response to these problems, the present invention provides a computer implemented method for enhanced security of color image using asymmetric RSA algorithm.

An aspect of the present disclosure relates to a computer implemented method is processed by at least one processor of at least one computing device, wherein the computing device has a memory storage and communicate module, wherein the computer implemented method comprising steps of Reading an input color image via a memory or from a visual input sensor; Converting the input color image into a gray scale image; Generating key by RSA algorithm, by selecting of two large prime numbers as a private key, with an auxiliary value, as the public key, wherein the public key is used to encrypt a message, and private key is used to decrypt a message or information; Computing the n value, n = pq,

wherein n is used as the modulus for both the public and private keys; Computing an Euler's totient function wherein Euler's totient function. This value is kept private; Selecting an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime, wherein e is the released as the public key; Determine d as $d \equiv e{-}1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$); Performing an encryption by transmiting public key (n, e) to keeps the private key d secret; and Performing the deencyption by recover m from c by using private key exponent d via computing. Given m, she can recover the original message M by reversing a padding scheme.

.

OBJECTIVE OF THE INVENTION

The principle objective of the present invention is to provide a computer implemented method for enhanced security of color image using asymmetric RSA algorithm.

Further objective of the present invention is to solve the problems in security in the transmission of color image presented in the prior art.

Another objective of the present invention is to present a way of encryption and decryption of digital color image using a RSA algorithm.

BRIEF DESCRIPTION OF DRAWINGS

Further clarify various aspects of some example embodiments of the present invention, a more particular description of the invention will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. It is appreciated that these drawings depict only illustrated embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the use of the accompanying drawings.

In order that the advantages of the present invention will be easily understood, a detailed description of the invention is discussed below in conjunction with the appended drawings, which, however, should not be considered to limit the scope of the invention to the accompanying drawings, in which:

Figure 1 shows the flow diagram representation of a computer implemented method for enhanced security of color image using asymmetric RSA algorithm, according to the present invention.

.

DETAIL DESCRIPTION

The present invention disclosures a computer implemented method for enhanced security of color image using asymmetric RSA algorithm.

Figure 1 shows the flow diagram representation of computer implemented method for enhanced security of color image using asymmetric RSA algorithm, according to the present invention.

Although the present disclosure has been described with the purpose of maintaining medical data and establishing an interactive communication between a plurality of users over a network, it should be appreciated that the same has been done merely to illustrate the invention in an exemplary manner and to highlight any other purpose or function for which explained structures or configurations could be used and is covered within the scope of the present disclosure.

Embodiments of the present disclosure include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware, and/or by human operators.

Although the present disclosure has been described with the purpose of implemented method for enhanced security of color image using asymmetric RSA algorithm , it should be appreciated that the same has been done merely to illustrate the invention in an exemplary manner and to highlight any other purpose or function for which explained structures or configurations could be used and is covered within the scope of the present disclosure.

The computer implemented method for enhanced security of color image using asymmetric RSA algorithm, is processed by at least one processor of at least one computing device, wherein the computing device has memory storage and communicate module.

The computer implemented method comprising steps of as first step of reading an input color image via a memory or from a visual input sensor. Then the image is converted into a gray scale image.

The public and private keys are generated by an RSA algorithm, wherein the RSA algorithm is processed by at least one processor of the computing device. It is performed by selecting of two large prime numbers as a private key, with an auxiliary value, as the public key, wherein the public key is used to encrypt a message, and private key is used to decrypt a message or information

The processer preform computing of the n value, n = PQ, wherein n is used as the modulus for both the public and private keys and computing an Euler's totient function wherein Euler's totient function. This value is

kept private. The integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primarily testing.

An integer e such is selected by the processor that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime, wherein e is the released as the public key.

A variable d is calculated by as $d \equiv e{-}1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$). Then an encryption is performed by transmitting public key (n, e) to keeps the private key d secret. Wherein in the step of encryption, first turns M into an integer m, such that $0 \leq m < n$ and gcd (m, n) = 1. Then it computes the cipher text c.

The decryption is performed by recover m from c by using private key exponent d via computing. Given m, she can recover the original message M by reversing a padding scheme. The encrypted image of the input color image differ then the input color image , & the decrypted image which is same as the original image from the encrypted image.

Embodiments of the present disclosure may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor

memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

The term "computing device" or "computer-readable storage medium" includes, but is not limited to, portable or non-portable storage devices, optical storage devices, and various other mediums capable of storing, containing, or carrying instruction(s) and/or data. A machine-readable medium may include a non-transitory medium in which data can be stored, and that does not include carrier waves and/or transitory electronic signals propagating wirelessly or over wired connections. Examples of a no transitory medium may include but are not limited to, a magnetic disk or tape, optical storage media such as compact disk (CD) or versatile digital disk (DVD), flash memory, memory or memory devices.

..

. .

Balram Singh

Patent Agent **IN/PA/2661**

Agent for Applicant

Dated 20th Day of Jan., 2020

CLAIMS

I/We claim:

1. A computer implemented method for enhanced security of color image using asymmetric RSA algorithm, the computer implemented method is processed by at least one processor of at least one computing device, wherein the computing device has a memory storage and communicate module, wherein the computer implemented method comprising steps of:

Reading an input color image via a memory or from a visual input sensor;

Converting the input color image into a gray scale image;

Generating key by RSA algorithm, by selecting of two large prime numbers as a private key, with an auxiliary value, as the public key, wherein the public key is used to encrypt a message, and private key is used to decrypt a message or information;

Computing the n value, n = PQ, wherein n is used as the modulus for both the public and private keys;

Computing an Euler's totient function wherein Euler's totient function. This value is kept private;

Selecting an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime, wherein e is the released as the public key;

Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$);

Performing an encryption by transmitting public key (n, e) to keeps the private key d secret; and

Performing the deencyption by recover m from c by using private key exponent d via computing. Given m, she can recover the original message M by reversing a padding scheme.

2. The computer implemented method for enhanced security of color image using asymmetric RSA algorithm as claimed in claim 1, wherein in the step of encryption , first turns M into an integer m, such that $0 \leq m < n$ and $\gcd(m, n) = 1$. Then it computes the cipher text c.

3. The computer implemented method for enhanced security of color image using asymmetric RSA algorithm as claimed in claim 1, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primarily testing.

4. The computer implemented method for enhanced security of color image using asymmetric RSA algorithm as claimed in claim 1, wherein the encrypted image of the input color image differ then the input color image , & the decrypted image which is same as the original image from the encrypted image.

.

.

.

.

Balram Singh
Patent Agent **IN/PA/2661**
Agent for Applicant
Dated 20th Day of Jan., 2020

COMPUTER IMPLEMENTED METHOD FOR ENHANCED SECURITY OF COLOR IMAGE USING ASYMMETRIC RSA ALGORITHM

ABSTRACT

The present invention is related to computer implemented method for enhanced security of color image using asymmetric RSA algorithm. The objective of present invention is to solve the anomalies presented in the prior art techniques related to security of color image using asymmetric RSA algorithm. It is disclosed in the disclosure that image files are encrypted and decrypted using RSA algorithm to improve the security before transferring/ receiving them in/from the communication channel. An image file is selected to perform encryption and decryption using key generation technique to transfer the data from one destination to another. This approach provides high security and it will be suitable for secured transmission of images over the networks or Internet.

Balram Singh
Patent Agent **IN/PA/2661**
Agent for Applicant
Dated 20th Day of Jan., 2020

DRAWINGS

Applicants**: Dr. Babu Rao Markapudi & Others** Sheet No. 1 Total 1

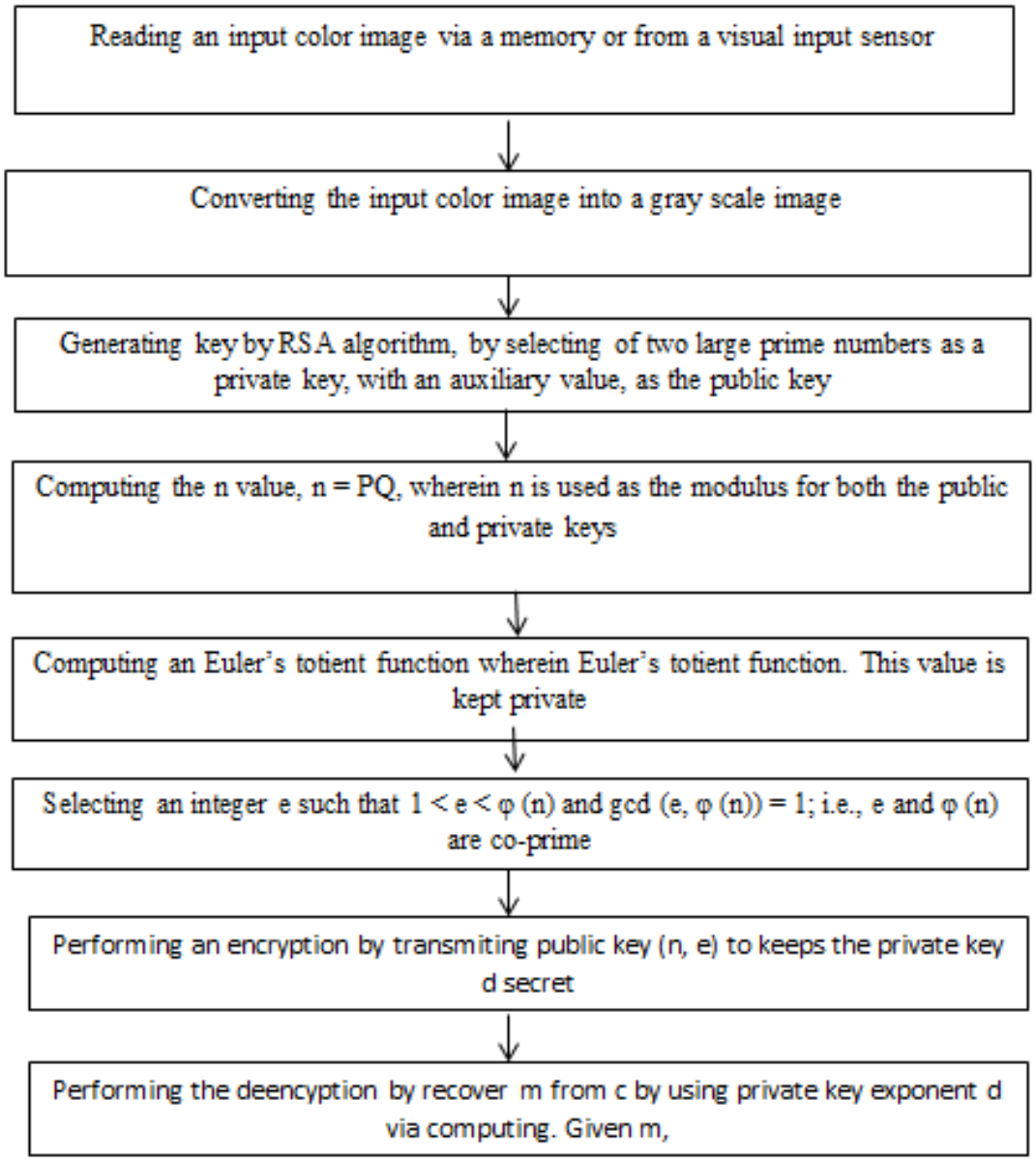

FIGURE 1

Balram Singh
Patent Agent **IN/PA/2661**
Agent for Applicant
Dated 17th Day of Jan.., 2020