New Encryption System Architecture for Image Transmission

Tomoyuki Nagase, Takashi Araki, Atsushi Watanabe and Hiroyuki Otsuki

Department of Electronic and Information System Engineering
Faculty of Science and Technology, Hirosaki University, 036-8561, Japan
nagase@cc.hirosaki-u.ac.jp

ABSTRACT

The security issue for delivering sensitive digital multimedia contents confidentially such as images or video conferencing over vulnerable public networks is becoming of paramount importance. This issue includes protecting digital media from copying and eliminating the risk of eavesdropping. This paper introduces an innovative approach to encrypt digital media using a new paradigm of public key cryptography scheme, which is called a quadripartite public-key (QPK). We considered a private key as a unit quaternion which has an arbitrary quadruple of real numbers, while the public key has three different components which are constructed using a mathematical model called quaternion rotation matrix QRM to generate an indescribable key. The QRM is used as rotation operator in three-dimensional space, i.e. R³ to rotate and spread the contents of the image which has been sampled into groups of pixels in three-dimensional space.

Key Words: Quaternion, image processing, security, cryptography.

1. INTRODUCTION

Securing sensitive digital media over vulnerable channels is one of our ambitions and is a very challenging problem that needs to be considered to protect intellectual property from unauthorized access and use.

This paper implements a quaternion tool as an encryption technique by providing four encryption keys. These key’s parameters are independent coefficients that has a free rotation in a 3-dimensional coordinate system. Any rotation can be represented by either a set of Euler angles or a matrix, as shown in Fig.1 (a) (b). The rotation is used in this paper as a function to encrypt information such as images or a secure video stream. The original image or a frame of the video stream is sampled into groups of pixels where each group is organized into 3x3 matrix array. All elements in the group are rotated and spread in 3-D space using a quaternion rotation matrix (QRM) [1], also we can say matrix rotation operator. The QRM is designated to be as public key that can be sent over internet or public networks.

To construct the QRM, we need to define a secret key which is part of a quaternion. Quaternion q is a hyper-complex number that has a 4-tuple of real numbers and as an element of R⁴, that has two parts scalar (real) and vectors (imaginary) parts, q = (w, V), or q = (w, V), where and V are scalar and vector, respectively. Also we can write q as a basic algebraic form as q = w + xi + yj + zk, where w is scalar and i, j, k are standard orthonormal basis in R³, the scalars x, y, z are called the components of the quaternion. Using above secret key q, a quaternion rotation matrix Γ(q) can be constructed, that is used as a tool to rotate a group of elements which has been organized as 3x3 matrix arrays in 3-D space.

2. QUATERNION ROTATION MATRIX

A quaternion rotation matrix is used as a tool to rotate a group of elements which has been organized as 3x3 matrix array in 3-D space, where the elements of the group appear in stochastic manner.

Consider two quaternions q = (w, x, y, z) and P = (θ, a, b, c), where a vector (a, b, c) in R³ corresponds to a pure quaternion whose the real part is zero. We define the quaternion operator P_rot to be a rotation operator or a frame rotation in R³ then

P_rot = q⁻¹ P q

(1)
Where \( q^{-1} \) is inverse quaternion \( q \).

However, for given quaternion \( P \) and \( q \), there are two maps and depend on how rotation can be performed and depending as we multiply on left or right such as \( q_L \) or \( q_R \), respectively. The rotation of \( P \) (\( P_{rot} \)) is given by

\[
P_{rot} = P q_R = q_L P \tag{2}
\]

We shall consider the matrix representation of the maps

\[
Pq_R = Rmat(q_R)P, \quad q_L P = Lmat(q_L)P \tag{3}
\]

Then the rotation of the quaternion \( P \) is

\[
P_{rot} = q^{-1}Pq = Rmat(q) Lmat(q^{-1})P \tag{4}
\]

Therefore the matrix representations of the linear transformations \( q_R, q_L \), are, respectively

\[
q_L = \begin{pmatrix}
w & -z & y & x \\
z & w & -x & y \\
- y & x & w & z \\
- x & - y & - z & w
\end{pmatrix}
\tag{5}
\]

\[
q_R = \begin{pmatrix}
w & z & - y & x \\
-z & w & x & y \\
y & - x & w & z \\
- x & - y & - z & w
\end{pmatrix}
\]

From Eq. (4), the rotation factor is

\[
\Gamma(q) = Rmat(q) Lmat(q^{-1}) \tag{6}
\]

By using Eq. (5) and substitute in Eq. (4), then the rotation matrix is given by

\[
\Gamma(q) = \begin{pmatrix}
1 - 2 y^2 - 2 z^2 & 2 x y - 2 w z & 2 x z + 2 w y \\
2 x y + 2 w z & 1 - 2 z^2 - 2 x^2 & 2 y z - 2 w z \\
2 x z - 2 w y & 2 y z + 2 w z & 1 - 2 x^2 - 2 y^2
\end{pmatrix}
\tag{7}
\]

The above equation is called quaternion operator or quaternion rotation matrix by which any other quaternion can be rotated using this operator

3. SYSTEM DESCRIPTION AND MODELING

The quaternion rotation matrix in above equation (7) will be used as public key for encryption system called a Quadripartite Public Key (QPK). The secret key components have variable lengths that make the QPK an obscure component and will have peculiar features to provide secure ambience for data transmissions.

An image data is built in arrays of RGB pixels, and the encryption of the image data will be feeble if we perform rotation on pixel-base parameters. Therefore, the image data is arranged into groups of pixel, as shown in Fig. 2, and then rotation can be performed on these groups. Now, we want to see how the rotation of the data can be done using QRM; suppose that an original image \( IM \), as shown in Fig.2, is uniformly divided into segments or blocks, and each block has a 3x3 element say \( IM = \{ G_{13}, G_{12}, G_{11}, \ldots, G_{nn} \} \), where \( m \) and \( n \) are real integer by setting \( m = 3 \) and \( G \) is a group of elements. A particular block is also break up into sub-groups, say \( G_{ij} = \{ S_{ij}, S_{12}, S_{13}, \ldots, S_{mn} \} \), the sub-group \( S_{mn} \) is also breakup into other sub-groups and so on, as shown in Fig.2. Thus, the rotation matrix in Equation (7) is used to rotate all elements or data in a group or a sub-group, so that, \( M' = \Gamma(q) \times M \), where \( M \) represents a group or a sub-group and \( M' \) is the data that has been rotated by matrix rotation operator \( \Gamma(q) \).

Suppose \( M_1 \) is a 3x3 matrix of sub-groups of an image’s data, the rotation of \( M_1 \) is preformed using a rotation matrix and we may write

\[
M_1' = \Gamma(q) \times M_1 = \Gamma(q) \times \begin{pmatrix}
S_{11} & S_{12} & S_{13} \\
S_{21} & S_{22} & S_{23} \\
S_{31} & S_{32} & S_{33}
\end{pmatrix}
\tag{8}
\]

The data \( M_1' \) in Eq. 8 is spreading to 3-dimensional space with different distance. The rotation of the data is applied to all groups and sub-groups. In order to recover the image that has been sent by using the inverse rotation matrix \( \Gamma(q)^{-1} \) which is implemented and expressed as

\[
M = \Gamma(q)^{-1} \times M' \tag{9}
\]

The quaternion representation, henceforth, provides an intrinsic means for resilient encryption system because the quaternion, as we mentioned above, implies four integrated parameters (keys), independently.

These keys might be any function or any random number with a variable key’s lengths. If any key is implemented incorrectly than the system will fail to disentangle its encrypted signal.

As we mentioned above that \( w \), \( x \), \( y \), and \( z \) are independent and variable parameters. In order to perform encryption of the data, we introduce a Quaternion Key Order (QKO) which is used as a factor that is implemented in the rotation matrix \( \Gamma(q) \) in (7) to produce multiple rotations. This method is used to make the image data likes a random pattern. We can generate \( m=3^n \) quaternion key, where \( n \) is the order number.

The initial order (for \( n=0 \)) of quaternion key which is identical to the private key and represented as \( K_p=q_{00}=(w_{01}, x_{01}, y_{01}, z_{01}) \). Using the first order sub-keys, it’s possible to generate a second order sub-keys such as (\( q_{21}, q_{22}, q_{23}, \ldots, q_{26} \)). Obviously, we can generate myriad sub-keys and in any order such that QKO is 3 (\( q_{3n} \)) or 4 (\( q_{4n} \)), where \( (i=1, 2, 3, \ldots, 3^n) \) and \( (i=1, 2, 3, \ldots, 4^n) \), respectively. If we suppose \( n \) is the number of order then we be able to construct \( 3^n \) (\( n = 0, 1, 2, \ldots \)) sub-keys.
From above concept, creating innumerable sub-keys for encryption data stream strengthens the security of the system. A 3-group of sub-key is used to construct quaternion rotation matrix that will be a public key (QPK) of our encryption system. Section 4 demonstrates how the quaternion encryption can be performed using image.

Indeed, QPK is able to provide essential factors to determining the highest degree of security and allowing users to maintain secure data passage over vulnerable channel.

4. IMPLEMENTATION ISSUES

This section demonstrates how digital media could be encrypted using quaternion technology. As we mentioned above that the rotation matrix is composed of 3x3 parameters array, hence, that the data of the image should also be formed as 3x3 matrix array, as shown in Fig. 2.

In our experiment, an original image of 360x480 pixels has been considered, which is illustrated in Fig. 3 (a). Primarily, the secret key’s parameters (x, y, z) has been chosen randomly or any value in the range of 0.0000 to 1.0000. By also choosing QRM from 3x3 to 81x81 pixels using the rotation matrix in (7) and let the parameters value of w, x, y and z are substituted in (7) as $w = 0.8913$, $x = 0.7621$, $y = 0.4565$, $z = 0.0185$, respectively, to obtain the following result

![Fig. 2: Divided image into groups and sub-groups and implementing rotation process of a group of pixels](image)

$\times$: Quaternion Multiplication

Fig. 2: Divided image into groups and sub-groups and implementing rotation process of a group of pixels

![Fig. 3: Quaternion matrix rotation applied on the original image](image)

(a) Original, (b) First rotation, (c) Second rotation, (d) Third rotation, (e) fourth rotation, (f) sixth rotation.
The QRM in (10) is called first order rotation or \( QKO=1 \), also we can perform second or third order by taken the values of each column in (10) as \( x \), \( y \) and \( z \) which are substituted in (7) as new parameters. Thus, the columns of (10) will present new rotation matrices \( \Gamma(q_{11}) \), \( \Gamma(q_{12}) \) and \( \Gamma(q_{13}) \). After constructing QRM for a specific order, the image data is organized into groups of pixels and arranged them in to a matrix array. The data matrix is applied in (8) to be rotated and spread into 3-diannmetrical space. In this example, we implemented only first order rotation \( QKO=1 \). The encryption image is shown in Fig. 4 and the encryption data of a small part of the above image is shown in table 1.

\[
\begin{bmatrix}
1.1665 & 0.6628 & 0.8419 \\
0.7287 & 0.4216 & -1.3416 \\
-0.7855 & 1.3754 & 0.0056
\end{bmatrix}
\] (10)

5. DISCUSSIONS

The results have been obtained and evaluated. The encryption system of this work, the QPK has four parameters so far and we selected the parameters in the range of 0.000 to 1.000 and \( QKO=1 \). Therefore, one parameter has \( 2^{16} \) patterns, and for four parameters we will have \( 2^{64} \) patterns. Furthermore, for \( QKO=2 \), we will have \( 2^{128} \) patterns and for \( QKO=3 \) then we will have \( 2^{192} \) patterns and so on. In this example, we used small size values for secret keys, however, in a real system the secret key parameters should be variable and long size keys which make the decryption of the data extremely difficult and enable to eliminate the risk of eavesdropping, as shown in Fig. 5.

![Fig. 3: Original Image](image1.png)

![Fig. 4: Encrypted Image](image2.png)

6. CONCLUSIONS

In this paper, a new encryption technique based on quaternion presentation was presented. Quaternion is capable to provide a sensible encryption technique to protect sensitive information from all attempts to intercept and read them. A computer simulation has been performed to demonstrate the high efficiency of the proposed technique.

7. REFERENCES


